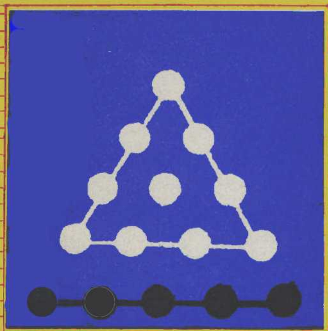
ZIRANSHUZHONG DEMINGZHU



自然数中的明珠

天津科学技术出版社

自然数中的明珠

俞晓群　编著

天津科学技术出版社

责任编辑：黄立民

自然数中的明珠
俞晓群 编著
•
天津科学技术出版社出版
天津市赤峰道130号
天津市马家店印刷厂印刷
新华书店天津发行所发行
•
开本787×1092毫米 1/32 印张5.125 字数108 000
1989年11月第1版
1989年11月第1次印刷
印刷：1—8 000
ISBN 7-5308-0453-7/O·26 定价：2.10元

目　　录

前　言

数学是自然科学的皇后，而数论是数学的皇后。

——高　斯

人们从幼儿时起，就开始认识自然数了。但是，您可曾知道：在这些“数”的字里行间，还蕴藏着一个无比瑰丽的世界……

记得有一位数学大师把数论中的问题比作一颗颗璀璨的明珠。当我们漫步在无垠的数学原野时，这些“明珠”便闪烁着奇异的光彩，仿佛向我们轻轻地呼唤着：来吧，朋友，这里遍布着无限的珍宝！出于欣喜和宠爱之情，笔者从这些五彩缤纷的明珠之中，信手择来八颗：完全数、亲和数、梅森数、……奉献给广大中学生和青年朋友，让我们共同分享这甘美的“人类智慧之果”！

本书详尽地介绍了数论中八种最重要的数字，全面地回顾了它们的产生、性质和发展史。从中可以概括地了解到数论的全貌，以及数论研究的思想方法。在从古至今的大量追述中，笔者力求史料翔实准确，侧重于发掘历代大数学家的思想过程。这对引导和激励青年一代步入艰深的数学领域，将会产生较好的效果。另外，本书是用历史叙述的形式写成的，它不是一部严格的数论教程，而是一个数学趣味性与知

识性高度相结合的读物。有鉴于此，书中关于数学性质的叙述是比较简略的，却注重于用大量的思想过程来引发人们的数学灵感。凡是具有初中以上文化程度的读者均可读懂。

在编写过程中，笔者曾得到南开大学数学研究所胡久稔先生的多次指教；尤其是得到了天津商学院吴振奎同志的鼎力协助和教诲，在此一并致谢！

俞晓群

1987年3月于沈阳

第一章 完 全 数

数学的使命就是在混沌之中去发现秩序。

——维 纳

§1.1 有趣的历史

完全数是自然数中最古老、最诱人的一类数字。它的定义是：一个数若等于它的全部因数之和（不包括自身），就叫做完全数。例如数字6的全部因数是1、2和3，它们的和恰好等于6，所以6是一个完全数。数字28的全部因数是1、2、4、7和14，它们的和恰好等于28，因此28是第二个完全数。

1．早期工作

人类对完全数的认识非常久远。古往今来，历代数学家都对它有着特殊的偏爱，因此，几乎每一个数字的产生都留下许多生动有趣的记载。现在，让我们从远古时代出发，浏览一下完全数的历史。

最早知道6和28的特性的是古印度人和希伯来人。但是，对于完全数比较深刻的认识是在古希腊时期。公元前约600年间，数字研究的先师毕达哥拉斯首先表述了他对完全数的酷爱，他说："6，象征着完满的婚姻以及健康和美丽，因为它的部分是完整的，并且其和等于自身"。公元前300年，欧几里得在他的巨著《几何原本》第九章中给出了一个关于完

全数的出色的定理。他写道：

命题6 若几何级数（从1开始）的一些项之和$1+2+2^2+\cdots\cdots+2^{n-1}$是素数，那么这个和同最末一项的乘积是一个完全数，即$(1+2+\cdots\cdots+2^{n-1})2^{n-1}$或$(2^n-1)2^{n-1}$是一个完全数。

验证一下：当$n=2$时，$2^2-1=3$是素数，而$(2^2-1)2^{2-1}=6$，果然得到了第一个完全数。欧几里得的工作开辟了完全数研究的先河。在古希腊文明泯灭之后，新的"数学王国"诞生在亚历山大城。公元100年，一位来自犹太给拉撒的阿拉伯人尼可马修斯写出一部卓越的数学著作《算术入门》。历史学家曾评价说：在数学领域中，这本书在算术方面的作用可以与欧几里得的《几何原本》媲美。书中尼可马修斯复述了欧几里得关于完全数的论述，并且将自然数划分为盈数、亏数和完全数三类，即一个自然数的全部因数（不包括自身）之和，若大于自身，就叫做盈数；若小于自身，就叫做亏数；若等于自身，就是完全数。例如，12的全部因数1、2、3、4和6之和等于16，大于12，所以12是盈数。8的全部因数1、2和4之和等于7，小于8，所以8是一个亏数。尼可马修斯正确地给出了四个完全数：

6，28，496，8128，

其中后两个是首次发现的。他深为完全数优美的性质所感染，在书中写道："奇迹发生了。正如世间缺少完美的事物，而丑陋的东西却比比皆是一样，自然数中遍布着杂乱无章的盈数和亏数；完全数却以它特有的性质熠熠发光，珍奇而稀少。"

几位数学大师的工作，以及他们对完全数的评估吸引了

众多的后来者。但是，自然数浩如烟海，完全数又如沧海一粟，在这渺渺茫茫的数海中，寻找千古珍稀的“数字珍珠”，谈何容易！在尼可马修斯之后，人们又经历了一千多年的探索，其间有著名数学家奥古斯丁、泰比特、伊本克拉、斐波那契等人的工作。结果，“上穷碧落下黄泉，两处茫茫皆不见”。时至1456年，正当人们迷惘之际，新的奇迹发生了。人们偶然发现，在一位无名氏的手稿中，竟神秘地给出了第五个完全数：33550336。这是一个具有八位数字的大数，它验证的艰巨性是可想而知的。但是，这位无名氏使用了什么方法？他为什么不愿披露自己的姓名？这些都使人们迷惑不解。

2. 梅森猜测

15世纪以来，由于大运算量的障碍，使许多著名学者在完全数的研究中屡受挫折。例如，16世纪意大利学者塔塔利亚错误地认为：当$n=2$和$n=3$至39的奇数时，$2^{n-1}(2^n-1)$是完全数。更有甚者是17世纪的庞格斯，他被人们称为“神数术”的大师。在他的一本近700页的著作《数的玄学》中，他一举列出了28个所谓“完全数”，其中除塔塔利亚给出的20个数字之外，他又补充了八个，最大的具有28位数字。但是，塔塔利亚和庞格斯都没有给出证明或解法，因此令人疑惑。

1603年，数学家克特迪历尽艰辛，最终严格地证明了：$2^{12}(2^{13}-1)=33550336$确是第五个完全数。并且正确地给出了第六和第七个完全数：$2^{16}(2^{17}-1)$和$2^{18}(2^{19}-1)$。但是，克特迪还错误地认为$2^{22}(2^{23}-1)$、$2^{28}(2^{29}-1)$和$2^{36}(2^{37}-1)$也是完全数，后来分别得到大数学家费尔

马和欧拉的指正。

可以说，在17世纪，完全数的研究出现了一个小高潮，而这个高潮的总结工作是由马林·梅森完成的。他在1644年指出：庞格斯给出的28个“完全数”中，只有8个是正确的，即当$n=2, 3, 5, 7, 13, 17, 19, 31$时，$2^{n-1}(2^n-1)$是完全数，它们分别位于庞格斯数表的第1、2、3、4、8、10、12和19位上（按数的位数排列）。梅森还认为：第九、第十和第十一个完全数是$2^{66}(2^{67}-1)$、$2^{126}(2^{127}-1)$和$2^{256}(2^{257}-1)$，并且，当$n\leqslant 257$时，只有这11个完全数。梅森知识广博、深为数学家们崇敬。他的上述论断竟统治了完全数研究近300年。不过有一点他同庞格斯一样，就是也没有给出他的证明或解法，他的工作只能算做一个“数学猜测”。

参与验证“梅森猜测”的有许多数学名流。例如，哥德巴赫认为梅森是对的；莱布尼兹曾错误地判断：只要n是素数，$2^{n-1}(2^n-1)$就是完全数。这些大数学家们也许是太轻视这些小数字了，结果屡屡出错。

3．欧拉定理

1730年，数学四伟人之一的欧拉思考了完全数的特性，果然出手不凡，给出一个出色的定理：

若P是一个偶完全数，则$P=2^{n-1}(2^n-1)$，其中n是某素数，2^n-1也是素数（证明见§1.2）。

这是欧几里得定理的逆定理。欧拉当时年仅23岁，正值风华之年，显示了他卓越的数学才能。但是，这一定理的证明一直没有发表，是人们在他的遗稿中发现的。欧拉也研究了梅森猜测，他指出：“我冒险断言：每一个小于50的素

数，甚至小于100的素数，使$2^{n-1}(2^n-1)$是完全数的仅有n取1，2，3，5，7，13，17，19，31，41，47。我从一个优美的定理出发得到了这些结果，我自信它们具有真实性。"可是，时过不久，欧拉本人及文森姆、蒲拉那分别证明了$n=41$和47时，不能得到完全数。看来，伟人的认识也有一个修正的过程。1772年，欧拉在致贝努利的一封信中说：他已严格地证实了$2^{30}\cdot(2^{31}-1)$是第8个完全数。他的方法是检验直至46339的素数，看$2^{31}-1$是否具有形如$248n+1$和$248n+63$的因数（详见本书§3.2）。此时，欧拉已双目失明。

欧拉的工作，使完全数的研究发生了深刻的变化。但是，人们仍然不能彻底解释梅森猜测，他的根据是什么？18世纪的数学家文森姆认为："梅森的基础或许是建立在他伟大的天赋之上，或许他认识到了更多的真理."

19世纪，人们对梅森的信任开始动摇了。首先，鲁卡斯创立了一种检验素数的新方法，并于1876年证明：$2^{66}(2^{67}-1)$不是完全数（首次发现了梅森的错误）。接着，鲁卡斯又证明：$2^{126}(2^{127}-1)$确是一个完全数.1883～1887年间，波佛辛等人证明了$2^{60}(2^{61}-1)$是一个完全数。1911～1914年，鲍尔等人证明了$2^{88}(2^{89}-1)$和$2^{106}\cdot(2^{107}-1)$也是完全数。最后，克劳契克与莱赫默分别在1922年与1931年证明了$2^{256}(2^{257}-1)$不是完全数。上述工作说明：梅森关于"$2^{66}(2^{67}-1)$、$2^{126}(2^{127}-1)$和$2^{256}(2^{257}-1)$是完全数"的猜测只有一个是对的；并且，在$n\leqslant257$的范围内，他丢掉了$n=61$，89，107时所产生的完全数。

至此，人们对完全数的研究告一段落。它说明，在电子计算机产生之前，繁重的运算量严重地限制了人们的认识进

程，即使在小小的完全数面前，也会让那些最优秀的数学家无计可施。这段关于完全数研究的历史也反映了数论的特点，正如数学家丹齐克所说：“数论是数学中所有部门里最最难的一门。不错，它的问题陈述出来，实在简单得连三尺孩童也能明白所讨论的是什么。但是，它所使用的方法却是那样的独特，必须有非凡的技巧和极大的敏才，才能找到恰当的入门之处.”

4．“上帝”引来的题外话

有趣的是完全数还受到一些“局外人”的厚爱，从而引出许多稀奇古怪的趣闻轶事。例如，远在中世纪，《圣经》的注释者就认为：完全数与上帝密不可分。他们引用《圣经》开篇“创世纪”中记载：上帝造物之始，第一天传播光明，第二天创造空气，第三天聚水成海，第四天日月经天，第五天游鱼飞雀，第六天塑造人类与走兽。这时，上帝完成了创造世界，开始了第七天的休息。并通过神学家之口说：“正是由于上帝造物用了6天，所以6才成了完全数。”《圣经》的注释者说：上帝创造的月亮周而复始一轮是28天，而28恰是第二个完全数。他们甚至把世界的混乱归咎于诺亚（《圣经》中的人物），说什么在洪水淹没世界之后，上帝第二次创造世界时，诺亚方舟上救得的是八个人，而不是六个人，所以世界不完美了。这些对于完全数的评注自然是十分荒唐的。中世纪著名学者奥古斯丁曾风趣地说：“6是自身完美的，这并非鬼使神差。”至于第二个完全数28与月行周期的关系，就更有些牵强。因为事实上月球绕地球运行一周只用了27.3天（即使按阴历算，一个月为29.5天）。

神学家们的荒诞注释反映了西方人对于完全数的崇拜。

例如 19世纪的意大利人还把数字6比作维纳斯，喻为美的象征。但是，这种“崇拜”也引来了一些哗众取宠的人。他们不顾数学的真实性，在那里信口开河，危言耸听。1936年3月27日，一则奇闻出笼了。世界著名的大通讯社——美联社就发布了一则题为《一个“新的完全数”》的消息：

一个具有155位数字的完全数被发现，一位博士用了5年的时间证明了欧几里得时代的问题

〔芝加哥3月26日美联社电〕 今天，克依格博士放下了他手中的笔和纸，并宣称：他已经证明了一个自欧几里得时代起，挫败了所有数学家的问题——找到了一个大于19位数字的完全数。

他说，一个完全数是等于它的因数之和的数。例如，28的和是1，2，4，7和14的和，所有这些数都可以整除28。克依格博士的完全数包含155位数字，即26815615859885194199148049996411692254957831641184786755447122887443528060146978161514511280138383284395055028465118831722842125059853682308859384882528256。

它的表达式为$2^{256}(2^{257}-1)$。博士说，在过去的5年中，他每天工作达17个小时，才证明了它是一个完全数。

这是一则错误百出的电文。首先，克依格的证明是错误的，$2^{256}(2^{257}-1)$不是完全数(莱赫默等人已经证实了这一点)。其次，数学家们已经找到了多个大于19位数字的完全数。这些常识性的错误几乎不值得真正的数学工作者们一驳。

5．完全数一览表

1946年，人类第一台电子计算机的产生，为寻找完全数带来盎然生机。但是，到1985年止，人们仅找到30个完全数，并且它们已经逐步失去昔日人们的宠爱，成为检验计算机功能或寻找“最大素数”的副产品。下面是已知的全部30个完全数，供读者欣赏。

表1·1　　　　　　　　完全数表

序号	n	完全数 $2^{n-1}(2^n-1)$	位数
1	2	$2(2^2-1)$	1
2	3	$2^2(2^3-1)$	2
3	5	$2^4(2^5-1)$	3
4	7	$2^6(2^7-1)$	4
5	13	$2^{12}(2^{13}-1)$	8
6	17	$2^{16}(2^{17}-1)$	10
7	19	$2^{19}(2^{19}-1)$	12
8	31	$2^{31-1}(2^{31}-1)$	19
9	61	$2^{61-1}(2^{61}-1)$	37
10	89	$2^{89-1}(2^{89}-1)$	54
11	107	$2^{107-1}(2^{107}-1)$	65
12	127	$2^{127-1}(2^{127}-1)$	77
13	521	$2^{521-1}(2^{521}-1)$	314
14	607	$2^{607-1}(2^{607}-1)$	366
15	1279	$2^{1279-1}(2^{1279}-1)$	770
16	2203	$2^{2203-1}(2^{2203}-1)$	1327
17	2281	$2^{2281-1}(2^{2281}-1)$	1373
18	3217	$2^{3217-1}(2^{3217}-1)$	1937
19	4253	$2^{4253-1}(2^{4253}-1)$	2561
20	4423	$2^{4423-1}(2^{4423}-1)$	2663
21	9689	$2^{9689-1}(2^{9689}-1)$	5834

续

22	9941	$2^{9941-1}(2^{9941}-1)$	5985
23	11213	$2^{11213-1}(2^{11213}-1)$	6751
24	19937	$2^{19937-1}(2^{19937}-1)$	12005
25	21701	$2^{21701-1}(2^{21701}-1)$	13066
26	23209	$2^{23209-1}(2^{23209}-1)$	13973
27	44497	$2^{44497-1}(2^{44497}-1)$	26789
28	86243	$2^{86243-1}(2^{86243}-1)$	51923
29	132049	$2^{132049-1}(2^{132049}-1)$	79501
30	216091	$2^{216091-1}(2^{216091}-1)$	30099

§1.2 特性种种

几千年来尽管神学家们给完全数蒙上了神秘的宗教色彩，完全数还是以它的数学性质放出奇异的光彩，在数学领域中吸引着后人。现在，让我们深入了解一下它的内容吧！

1．两个定理

上一节我们曾提到欧几里得和欧拉的工作。现在我们介绍一下他们完美的数学证明。为了叙述方便，我们先给出一些数论中常用符号的定义和二个性质。

定义 设m、n是自然数，则（1）$m \mid n$表示m整除n；$m \nmid n$表示m不能整除n。（2）$(m, n)=1$表示m和n互素，即m和n的公因数只有1。（3）$\sigma(n)$表示n的全部因数之和。例如，$\sigma(6)=1+2+3+6=12$。

性质1 n是完全数的充要条件是$\sigma(n)=2n$。这一引理

可由完全数的定义立即推出。

性质2 若$(m, n)=1$，则$\sigma(mn)=\sigma(m)\cdot\sigma(n)$。

证明 首先，对于任一自然数$m(\neq 1)$，推出$\sigma(m)$的一个表达式。设m的素因数分解是$m=p_1^{a_1}\cdots p_k^{a_k}$，则对于任一$d\mid m$，有$d=p_1^{b_1}\cdots p_k^{b_k}$，其中$0\leqslant b_i\leqslant a_i(i=1,\cdots,k)$。显然，它们恰好是乘积$(1+p_1+\cdots+p_1^{a_1})(1+p_2+\cdots+p_2^{a_2})\cdots(1+p_k+\cdots+p_k^{a_k})$的展开式中的各项，所以这个展式就等于$\sigma(m)$。而式中的每一个括号内都是一个几何数列，所以$\sigma(m)=\dfrac{p_1^{a_1+1}-1}{p_1-1}\cdots\dfrac{p_k^{a_k+1}-1}{p_k-1}$。

现在，设m和n的素因数分解是$m=p_1^{a_1}\cdots p_k^{a_k}$，$n=q_1^{b_1}\cdots q_t^{b_t}$，因为$(m, n)=1$，所以$p_i\neq q_j(i-1, 2, \cdots k; j=1, 2, \cdots, t;)$。因此，$m\cdot n=p_1^{a_1}\cdots p_k^{a_k}\cdot q_1^{b_1}\cdots q_t^{b_t}$。根据前面的推导有$\sigma(m\cdot n)=\dfrac{p_1^{a_1}-1}{p_1-1}\cdots\dfrac{p_k^{a_k}-1}{p_k-1}\cdot\dfrac{q_1^{b_1}-1}{q_1-1}\cdots\dfrac{q_t^{b_t}-1}{q_t-1}$。它显然等于$\sigma(m)\cdot\sigma(n)$。

注 具有这种性质的函数叫做积性函数。引理2的证明思路十分简洁，但符号比较复杂。读者也可以牢记结果，略读证明过程。

欧几里得定理 若2^n-1是素数，则$2^{n-1}(2^n-1)$是一个完全数。

注 我们先给出一种极初等的证法（这也可能是古希腊人的思想方法），然后再给出一种简洁的证法。

证法一 设$P=2^{n-1}(2^n-1)$，其中2^n-1是一个素数。显然，P的全部因数是$1, 2, 2^2, \cdots 2^n$及$2^n-1, 2(2^n-$

1），…，$2^{n-1}(2^n-1)$，它们的和$1+2+2^2+\cdots+2^{n-1}+(1+2+\cdots+2^{n-1})(2^n-1)=2^n(1+2+\cdots+2^{n-1})$。而几何数列$S=1+2+\cdots+2^{n-1}=2^n-1$，所以$P$的全部因数之和（包括自身）等于$2^n(2^n-1)=2[2^{n-1}(2^n-1)]=2P$。因此$P$是一个完全数。

证法二 注意到$(2^{n-1}, 2^n-1)=1$，则$\sigma(P)=\sigma(2^{n-1}(2^n-1))=\sigma(2^{n-1})\sigma(2^n-1)$。而$\sigma(2^{n-1})=2^n-1$，$\sigma(2^n-1)=2^n$，所以$\sigma(P)=2^n(2^n-1)=2P$。由引理1，$P$是一个完全数。

欧拉定理 若P是一个偶完全数，则$P=2^{n-1}(2^n-1)$其中n是某素数，2^n-1也是素数。

注 对此，我们也给出两种证法，其中的第一种方法是迪克森（名著《数论史》的作者）在1911年给出的，第二种方法是在欧拉的遗稿中发现的。

证法一 设P为偶完全数，且$P=2^n m$，显然m是奇数且$n>1$。由于$\sigma(m)>m$，设$\sigma(m)=m+s$，其中$s>0$。显然$(2^n, m)=1$，所以$\sigma(p)=\sigma(2^n m)=\sigma(2^n)\cdot\sigma(m)=(2^{n+1}-1)(m+s)$。又因为$p$是完全数，所以$\sigma(p)=2p=2^{n+1}m$。因此$2^{n+1}m=(2^{n+1}-1)(m+s)$。整理得$m=(2^{n+1}-1)s$。这说明$s$是$m$的一个因数，$s<m$。但$\sigma(m)=m+s$，所以$s$是$m$的全部因数（不包括$m$）之和，即若$m$的全部因数为1，$d_1$，$d_2$，…，$d_k$，则$s=1+d_1+\cdots+d_k$。又因为$s$也是$m$的一个因数，由此可推出$s$只能等于1，所以$m=(2^{n+1}-1)s=2^{n+1}-1$，且$\sigma(m)=m+s=m+1$。由此可知$m$是一个素数，进而可知$n+1$也是一个素数。

证法二 设$P=2^n m$是完全数，m为奇数。P的各因数之

和$(2^{n+1}-1)\sigma(m)$应等于$2P$，因而有$m/\sigma(m)=(2^{n+1}-1)/2^{n+1}$，它是一个既约分数，因此对于某整数$c$有$m=(2^{n-1}-1)c$。若$c=1$，则$m=2^{n+1}-1$为素数（因为$\sigma(m)=2^{n+1}$）；若$c>1$，则$\sigma(m)\geqslant m+(2^{n+1}-1)+c+1$。于是，$\sigma(m)/m\geqslant 2^{n+1}(c+1)/m>2^{n+1}/(2^{n+1}-1)$。出现矛盾。

注 欧拉的证明十分简洁，但是他略去了一些细节和说明。有兴趣的读者可自己补全。

2．八个性质

完全数有许多优美的性质，现列举如下：

（1）每一个偶完全数的末位数字均为6或8；若为8，则倒数第二位数字一定为2。

这一性质是由尼可马修斯给出的。他还认为：完全数以6和8交错地结尾，并且每一级位数中都有一个完全数。这后两个观点都是错误的，例如，第五个完全数33550336与第六个完全数8589869056的尾数都是6。又如，第四个完全数具有四位数字，而第五个完全数具有八位数字，它们并非处于连续的位数之中。

（2）除6之外，任何偶完全数除以9均余1。

这一性质是由塔塔利亚发现的。他同时还错误地认为：数列1＋2＋4，1＋2＋4＋8，…交替给出素数与合数。

（3）除6之外，所有偶完全数的数字根等于1，即它们各个位上的数字和逐次累加，最终等于1。例如：

28：2＋8＝10，1＋0＝1；

496：4＋9＋6＝19，1＋9＝10，1＋0＝1；

8128：$8+1+2+8=19$，$1+9=10$，$1+0=1$。

(4) 每一个偶完全数都是一个六角形数，因此也是一个三角形数，即可以表示成$1/2n(n+1)$的形式（$n\geq 3$）。

例如：

$n=3$时，$1/2[3(3+1)]=6$；

$n=7$时，$1/2[7(7+1)]=28$；

$n=31$时，$1/2[31(31+1)]=496$。

（三角形数和六角形数的定义见本书第八章形数）。这个性质是1575年间，由数学家默热勒克斯给出的。

(5) 除6之外，每一个偶完全数$2^{n-1}(2^n-1)$是从1开始的奇数的立方和，这里奇数的个数等于$2^{(n-1)/2}$。

例如：

$28=1^3+3^3$；　　$496=1^3+3^3+5^3+7^3$；

$8128=1^3+3^3+\cdots+15^3$。

(6) 每一个偶完全数$2^{n-1}(2^n-1)$是从2^{n-1}到2^{2n-2}的2的连续方幂之和。

例如：

$6=2^1+2^2$；　　$28=2^2+2^3+2^4$；

$496=2^4+2^5+2^6+2^7+2^8$。

(7) 每一个偶完全数的全部因数的倒数之和都等于2。

例如：

6：$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=2$；

28：$\frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\frac{1}{7}+\frac{1}{14}+\frac{1}{28}=2$；

496：$\frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\frac{1}{31}+\frac{1}{62}+\frac{1}{124}+\frac{1}{248}+\frac{1}{496}$

$=2$。

（8）每一个偶完全数都可以写成从1开始的连续自然数之和。

例如：

$6=1+2+3$；　　　　$28=1+2+\cdots+7$；

$496=1+2+\cdots+31$；　　$8128=1+2+\cdots+127$。

这一性质是1652年由布热瑟恩斯证明的。

对于上述性质，我们仅给出（3）的证明，其余的可由读者演习。

证明　由于每一个偶完全数均可表为$2^{n-1}(2^n-1)$，而根据几何数列的性质$2^n-1=1+2+\cdots+2^{n-1}$，所以完全数$P=2^{n-1}+2^n+\cdots+2^{2n-2}$，即每一个偶完全数都可以表成从$2^{n-1}$到$2^{2n-2}$的2的连续方幂之和。

3．一些推广

数学研究的一个重要方面，就是进行从特殊到一般、从低维到高维的推广。由此常常会产生许多重要的数学发现。对于完全数的推广，是十分丰富有趣的，现略述如下：

（1）多倍完全数：对于自然数n，如果$\sigma(n)=kn$，k为自然数，则称n为k倍完全数。一般表示成$P_k^{(i)}$的形式，其中k是这个完全数的倍数；i表示在同一倍数的完全数中，它被发现的序号。显然，我们前面论述的完全数是二倍完全数，即$P_2^{(1)}=6$，$P_2^{(2)}=28$，$P_2^{(3)}=496$，…。1557年，数学家

伊克德发现：120的全部因数之和是1+2+3+4+5+6+8+10+12+15+20+24+30+40+60+120=360=3·120，即等于自身的三倍。这是多倍完全数的最早研究。1631年，梅森在致笛卡尔的一封信中明确指出：存在着$k>2$的多倍完全数，第一个3倍完全数就是$P_3^{(1)}=120$。梅森的想法立即引起许多数学家的关注。5年后，费尔马兴奋地转告梅森，他终于找到了第二个P_3，即$P_3^{(2)}=672$。1638年4月，一位桀骜不驯的学者琼米向笛卡尔宣称：他找到了$P_3^{(3)}=523776$。并向厄笛卡尔挑战："试问第四个三倍完全数是什么？"两个月后，笛卡尔请梅森转告琼米厄，他已轻松地找到$P_3^{(4)}=1476304896$。

一个月后，笛卡尔又以他超人的天赋一举给出六个4倍完全数，以及一个5倍完全数。同年11月，笛卡尔在致梅森的一封信中说："他所以能得到如此丰富的结果，是因为发现了几个关于多倍完全数迷人的性质。即

①如果n是一个P_3数，并且不是3的倍数，则$3n$是P_4数。

②如果一个P_3数可以被3整除，但是既不能被5也不能被9整除，则$45P_3$是P_4数。

③如果一个P_3数可以被3整除，但是不能被7、9或13整除，则$3\cdot7\cdot13\cdot P_3$是P_4数。

④如果n不是3的倍数，并且如果$3n$是一个P_{4k}数，则n是一个P_{3k}数。

注 这些性质的证明都不困难，现仅给出①的证明：

由于n是P_3数，则$\sigma(n)=3n$。又因为n不是3的倍数，所以$(n,3)=1$。从而$\sigma(3n)=\sigma(3)\cdot\sigma(n)=4\sigma(n)$。由于$\sigma(n)=3n$，所以$\sigma(3n)=\sigma(3)\cdot\sigma(n)=4(3n)$，即$3n$是$P_4$数。

笛卡尔的工作开阔了人们的研究视野，此后几百年间（直至电子计算机产生），数学家们通过繁冗的笔算找到许多多倍完全数。限于篇幅，我们取主要结果列表如下（时间：16世纪～20世纪初）：

表1·2　　多倍完全数表

	发现序数i	P_k	发现者	年代
$P_3^{(i)}$	1	$120=2^3\cdot 3\cdot 5$	伊克德	1557
	2	$672=2^5\cdot 3\cdot 7$	费尔马	1636
	3	$523776=2^9\cdot 3\cdot 11\cdot 31$	琢米厄	1638
	4	$2^{13}\cdot 3\cdot 11\cdot 43\cdot 127$	笛尔卡	1638
	5	$2^8\cdot 5\cdot 7\cdot 19\cdot 37\cdot 73$	梅　森	1639
	6	$2^{14}\cdot 5\cdot 7\cdot 19\cdot 31\cdot 151$	费尔马	1643
$P_4^{(i)}$	1	$2^5\cdot 3^3\cdot 5\cdot 7$	笛卡尔	1638
	2	$2^3\cdot 3^2\cdot 5\cdot 7\cdot 13$	笛卡尔	1638
	3	$2^9\cdot 3^3\cdot 5\cdot 11\cdot 31$	笛卡尔	1638
	4	$2^9\cdot 3^2\cdot 7\cdot 11\cdot 13\cdot 31$	笛卡尔	1638
	5	$2^{13}\cdot 3^3\cdot 5\cdot 11\cdot 43\cdot 127$	笛卡尔	1638
	6	$2^{13}\cdot 3^2\cdot 7\cdot 11\cdot 13\cdot 43\cdot 127$	笛卡尔	1638
	7	$2^8\cdot 3\cdot 5\cdot 7\cdot 19\cdot 37\cdot 73$	梅　森	1639
	8	$2^7\cdot 3^3\cdot 5^2\cdot 17\cdot 31$	梅　森	1639
	9	$2^{10}\cdot 3^3\cdot 5^2\cdot 23\cdot 31\cdot 89$	梅　森	1639
	10	$2^{14}\cdot 3\cdot 5\cdot 7\cdot 19\cdot 31\cdot 151$	费尔马	1643
	11	$2^7\cdot 3^6\cdot 5\cdot 17\cdot 23\cdot 137\cdot 547\cdot 109$①	费尔马	1643
	12	$2^2\cdot 3^2\cdot 5\cdot 7^2\cdot 13\cdot 19$	D.N莱赫默	1900
	13	$2^8\cdot 3^2\cdot 7^2\cdot 13\cdot 19^2\cdot 37\cdot 73\cdot 127$	D.N莱赫默	1900
	14	$2^{14}\cdot 3^2\cdot 7^2\cdot 13\cdot 19^2\cdot 31\cdot 127\cdot 151$	卡米切尔	1906
	15	$2^{25}\cdot 3^3\cdot 5^2\cdot 19\cdot 31\cdot 683\cdot 2731\cdot 8191$	卡米切尔	1906
	16	$2^{25}\cdot 3^6\cdot 5\cdot 19\cdot 23\cdot 137\cdot 547\cdot 683$ $\times 1093\cdot 2731\cdot 8191$	卡米切尔	1906

注　①$P_5^{(4)}$最早出现在梅森在1639年给出的“多倍完全数表”中，但大概由于印刷原因错了一个数字，1900年由莱赫默指正。

续

$P_5^{(i)}$	1	$2^7\cdot3^4\cdot5\cdot7\cdot11^3\cdot17\cdot19$	笛卡尔	1638
	2	$2^{10}\cdot3^5\cdot5\cdot7\cdot13\cdot19\cdot23\cdot89$	福兰尼克尔	1638
	3	$2^7\cdot3^5\cdot5\cdot7^2\cdot13\cdot17\cdot19$	笛卡尔	1638
	4	$2^{11}\cdot3^3\cdot5^2\cdot7^2\cdot13\cdot19\cdot31$	梅　森	1639
	5	$2^{20}\cdot3^3\cdot5\cdot7^2\cdot13^2\cdot19\cdot31\cdot61\cdot127\cdot337$	费尔马	1643
	6	$2^{17}\cdot3^5\cdot5\cdot7^3\cdot13\cdot19^2\cdot37\cdot73\cdot127$	费尔马	1643
	7	$2^{10}\cdot3^4\cdot5\cdot7\cdot11^2\cdot19\cdot23\cdot89$	鲁卡斯	1877
	8	$2^{21}\cdot3^6\cdot5^2\cdot7\cdot19\cdot23^2\cdot31\cdot79\cdot89\cdot137$ $\times547\cdot683\cdot1093$	D.N莱赫默	1900
$P_6^{(i)}$	1	$2^{23}\cdot3^7\cdot5^3\cdot7^4\cdot11^3\cdot17^2\cdot31\cdot41\cdot61$ $\times241\cdot307\cdot467\cdot2801$	费尔马	1643
	2	$2^{27}\cdot3^5\cdot5^3\cdot7\cdot11\cdot13^2\cdot19\cdot29\cdot31\cdot43$ $\times61\cdot113\cdot127$	费尔马	1643
	3	$2^{36}\cdot3^8\cdot5^5\cdot11\cdot13^2\cdot19\cdot31^2\cdot43$ $\times61\cdot83\cdot223\cdot331\cdot379\cdot601\cdot757$ $\times1201\cdot7019\cdot823543\cdot616318177$ $\times100895598169$	费尔马	1643
	4	$2^{19}\cdot3^6\cdot5^3\cdot7^2\cdot11\cdot13\cdot19\cdot23\cdot31\cdot41$ $\times137\cdot547\cdot1093$	D.N莱赫默	1900
	5	$2^{24}\cdot3^3\cdot5\cdot7^2$ 11·[illegible]3·17·19[illegible]·31·43 $\times53\cdot127\cdot379\cdot601\cdot757\cdot189$	D.N莱赫默	199
	6	$2^{[illegible]1}\cdot(2^{62}-1)\cdot3^7\cdot5^4\cdot7^2\cdot11\cdot13\cdot19^2$ $\times23\cdot59\cdot71\cdot79\cdot127\cdot157\cdot379\cdot757$ $\times43331\cdot3033169$	卡恩尼佛姆	1902
	7	$2^{15}\cdot3^5\cdot5^2\cdot7^2\cdot11\cdot13\cdot17\cdot19\cdot31\cdot43\cdot257$	卡米切尔	1906
$P_7^{(i)}$	1	$2^{46}\cdot3^{15}\cdot5^3\cdot7^5\cdot11\cdot13\cdot17\cdot19^4\cdot23\cdot31$ $\times37\cdot41\cdot43\cdot61\cdot89\cdot97\cdot151\cdot193$ $\times911\cdot2351\cdot4513\cdot442151$ $\times13264529$	卡恩尼佛姆	1902

②在1877年鲁卡斯给出的$p_5^{(7)}$中，将“7”写为“7^2”。1906年由卡米切尔指正。

这是一张令人感慨的数表，它是单凭笔算产生的，其中不知凝聚着历代数学家多少血汗！

另外，本世纪初，数学家莱赫默还给出一个关于多倍完全数的重要性质：一个P_3数至少包含三个不同的素因数；一个P_4数至少包含四个不同的素因数；一个P_5数至少包含六个不同的素因数；一个P_6数至少包含九个不同的素因数；一个P_7数至少包含14个不同的素因数。

(2) 半完全数与怪数：对于自然数n，如果它是自己的某些因数的和，就称做半完全数。例如，12=6+4+2，所以它是一个半完全数。显然，半完全数必是盈数。不是半完全数的盈数很少见，因此称为怪数。现已知的三个最小的怪数是70、836和4030。迄今尚未发现任何奇数怪数。数学家厄尔迪什曾悬赏10美元求第一个奇数怪数；悬赏25美元最先证明不存在奇数怪数。但是后来的研究证明：怪数是无限多的。

(3)乘积完全数：对于自然数n，它的全部因数（不包括自身）的乘积等于自身的乘幂，就叫做乘积完全数。见表1.3。

表1·3　　乘积完全数表

数n	n的因数之积
12	$1\cdot2\cdot3\cdot4\cdot6=144=12^2$
20	$1\cdot2\cdot4\cdot5\cdot10=400=20^2$
45	$1\cdot3\cdot5\cdot9\cdot15=1225=45^2$
24	$1\cdot2\cdot3\cdot4\cdot6\cdot8\cdot12=13824=24^3$
40	$1\cdot2\cdot4\cdot5\cdot8\cdot10\cdot20=64000=40^3$
48	$1\cdot2\cdot3\cdot4\cdot6\cdot8\cdot12=5308416=48^4$
80	$1\cdot2\cdot4\cdot5\cdot8\cdot10\cdot16\cdot20\cdot40=40960000=80^4$
405	$1\cdot3\cdot5\cdot9\cdot15\cdot27\cdot45\cdot81\cdot135=26904200625=405^4$

还有一些数字，人们把它们冠以“几乎完全数”、“强力完全数”等名目，但是距离“完全”二字愈来愈远，所以在此就不一一列举了。

§1.3 待揭之谜

对小小的完全数，人们大概觉得对它的认识已经完美无瑕了。其实不然，还有许多关于完全数的猜想人们无法解释。有些问题人们至今还无从下手。本节我们将着重介绍一下奇数完全数的研究。

细心的读者大概早已发现，我们在前面介绍的完全数都是偶数。是否存在奇数完全数呢？这至今还是一个谜。但是，对于奇数完全数的研究却十分久远。1638年11月，笛卡尔在致梅森的一封信中首次开创奇数完全数的研究。他认为：每一奇数完全数必具有pQ^2的形式，其中p是素数。笛卡尔坚信不久即会找到奇数完全数，但始终未能如愿。1657年，福兰尼克尔认为：笛卡尔给出的pQ^2中，p是形如$4n+1$的素数。1774年间，欧拉进一步给出一个关于奇数完全数的定理，现引述如下：

奇数完全数定理 任何奇数完全数必为$p^{4a+1}\cdot Q^2$，其中p为奇素数，a和Q是自然数。

证明 设$n=P_1P_2\cdots P_k$是将n分解为不同奇素数幂的表示式。令$Q=\sigma(P_i)$，$i=1,2,\cdots,k$，。若$\sigma(n)=2n$，则$2P_1P_2\cdots P_k=Q_1Q_2\cdots Q_k$。因此，$Q_1$、$Q_2$、…、$Q_k$中有一数，不妨设为$Q_1$，是一个奇素数的2倍，而其余各数均为奇数。故$P_2$、$P_3$、…、$P_k$是素数的偶次幂，而$P_1=p^{4a+1}$，

p为某奇素数，a为自然数。

注 这段证明是欧拉一篇草稿的原文，叙述过于简单。有兴趣的读者可试补证。

上述工作曾使人们产生错觉似乎认为按照表达式 $P^{4a+1}\cdot Q^2$ 做适当的验证就可以找到奇数完全数了。结果事与愿违，数学家们逐步发现，若奇数完全数存在的话，它将大得惊人！例如：1908年图卡尼诺夫证明：每一个奇数完全数将不小于2000000。1963年，数学家奥尔在一篇文章中写道：“凯努德先生已经证明，不存在小于 1.4×10^{14} 的奇数完全数。最近，我的学生马斯凯特告诉我，他已经能够证明这个下限是 10^{18}。”奥尔的话反应了一个事实：随着人们对奇数完全数研究的深入，它存在的下限已在逐步增长。果然，1968年，塔克曼在IBM上宣布：他在1967年证明，如果奇数完全数存在，它必须大于 10^{36}。1972年，有人证明，奇数完全数必大于 10^{50}。1982年，有人证明，它必须大于 10^{120}。目前这个下限仍在增长。显然，寻找奇数完全数的前途十分渺茫。

不过，渺茫的原因并非仅限于此，人们还发现了众多的约束条件。下面列出其中几个，就足以令人望而却步。

(1) 1774年间欧拉认为：不存在形如 $4n+3$ 的奇数完全数（由利奈特（1879）、鲁卡斯（1891）等人证明）。

(2) 1844年间勒贝格认为：不存在少于4个不同素因数的奇数完全数（由迪什波夫斯（1878）证明）。1888年塞里外斯特认为：不存在少于6个不同素因数的奇数完全数(本世纪70年代得证）。1980年以后人们证明它将不少于八个不同的素因数。

(3)当奇数完全数除以12时，必余1；除以36时，必余9。

(4)在奇数完全数定理中，设$Q^2=q_1^{2a_1}\cdots q_n^{2a_n}$，$q_i$($i=1$，…，$n$)为任意奇素数．则如果除了$a_1$之外，所有的$a_i$都等于1，那么$a_1$不能等于2；如果除了$a_1$、$a_2$之外，所有的$a_i$都等于1，那么$a_1$和$a_2$不能等于2。

(5)按照(4)中的条件，如果所有的a_i都等于2，则N不是完全数。

(6)按照(4)中的条件，如果q_i的所有指数都加1，则得到的指数不能有公因子9、15、21或33。

(7)按照(3)中的条件，如果p的指数等于5，则所有的a_i都不等于1或2。

(8)1888年塞里外斯特证明：不能被3整除的奇数完全数最少有9个不同的素因数。后来有人证明：如果它不能被21整除，则至少有11个不同的素因数；不能被15整除，则至少有14个不同的素因数；不能被105整除，则至少有27个不同的素因数．这个条件使此类奇数完全数必须大于10^{44}。

(9)1887年间舍塞热证明：具有n个不同素因数的奇数完全数，它的最小因数不大于$n\sqrt{2}$。

(10)奇数完全数必形如$12m+1$或$36m+1$，其中m为素数。

(11)1975年有人证明：奇数完全数必有一个大于100110的素因数。

一种数字，尚不知其存在与否，就产生了如此众多的约束条件，堪称数学界的一大奇闻！

在本章结束之际，还有一个待揭之谜始终尾随着我们：完全数是有限个还是无限多的呢？这个问题就更难回答了，

正如宇宙是无限的一样，自然数也是无限的。谁能步入那无限的思维空间之中，成为人类的先行者？这真是太难了！

第二章 亲 和 数

人类智慧掌握着三把钥匙：一把开启数字，一把开启字母，一把开启音符。

——雨果

§2.1 从毕达哥拉斯谈起

亲和数的定义是：对于自然数m和n，若m的全部因数（不包括自身）之和恰好等于n，而n的全部因数（不包括自身）之和又恰好等于m，则m和n是一对亲和数。例如，220的全部因数之和$1+2+4+5+10+11+20+22+44+55+110=248$，而248的全部因数之和$1+2+4+71+142=220$，所以220和248是一对亲和数。

同完全数一样，亲和数也有一段漫长而有趣的历史。据史书记载：大约古印度人和希伯来人已经知道了亲和数。例如，出自希伯来文的《圣经》创世纪第三十二章第十四节中写道："人类的始祖雅各曾送给他的长兄伊绍200只母羊和20只公羊，以表达他内心的深情"。显然，母羊数与公羊数之和正好是亲和数对220和284中的一个。因此人们推测：希伯来人把亲和数做为一种吉兆。

但是，明确地给出亲和数的是毕达哥拉斯。有一段故事

写道：一次，毕达哥拉斯学派聚集在克罗托那城中，讨论“数字对于万物的作用”。一位学者问：“我结交朋友时，存在着数的作用吗？”毕达哥拉斯回答：“朋友是你灵魂的倩影，要象220和284一样亲密。”接着，毕氏讲解了亲和数性质，使那位学者惊呆了。因此，亲和数又有“友数”之称。

220和284是远古时期人们找到的唯一一对亲和数。在毕达哥拉斯之后的1500多年间，数学家们虽然进行了大量的工作，但是毫无收获。至公元9世纪，《天方夜谭》的故乡巴格达出现了一位伟大的博学者泰比特·依本克拉。他是一个异教徒，精于医学、哲学和天文学，并且酷爱数学。暇余之际，他对亲和数潜心思索，竟惊人地发现一个求亲和数的公式，现叙述如下：

泰比特·依本克拉公式　设$a=3\cdot2^n-1$，$b=3\cdot2^{n-1}-1$，$c=9\cdot2^{2n-1}-1$，这里n是大于1的正整数。则当a、b和c是大于2的素数时，2^nab和2^nc是一对亲和数。

证明　因为a、b和c是互异的素数，所以它们两两互素。又根据已知可证2^n与a、b、c均互素，所以$\sigma(2^nab)=\sigma(2^n)\sigma(a)\sigma(b)=2^{n+1}\cdot3\cdot2^n\cdot3\cdot2^{n-1}=9\cdot2^{3n}$，$\sigma(2^nc)=\sigma(2^n)\sigma(c)=2^{n+1}\cdot9\cdot2^{2n-1}=9\cdot2^{3n}$。因此$\sigma(2^nab)=\sigma(2^nc)$，显然$2^nab$与$2^nc$是一对亲和数。

注　根据$\sigma(x)$函数的定义，可知m和n是一对亲和数的充要条件是$\sigma(m)=\sigma(n)=m+n$。上述证明引用了这一结论。

验证一下：当$n=2$时，$a=11$，$b=5$，$c=71$，都是素数，而$2^nab=220$，$2^nc=284$，果然得到了第一对亲和数。这一公式原载于一部阿拉伯文的手稿中，1852年由沃伯克译成法

文，存于巴黎国家图书馆。

泰比特·依本克拉的工作并没有改变亲和数研究的困境，人们仍然没有找到新的亲和数。此后几百年间，一些著名的数学家，诸如16世纪的斯蒂弗尔、卡尔丹、庞格斯和塔塔利亚等人，甚至认为亲和数只有一对。还有一些无聊的世人，把这对亲和数视如珍宝，妄谈其魅力之深，作用之大。例如，一位11世纪的阿拉伯学者麦兹克伊特在其著作中详述了用亲和数预测婚姻的方式。大意是：在择婚之际，分别点出220和284块糖果，让男女双方吃，以吃尽或吃得多少来确定姻缘和恩爱程度。这种“把戏”流传极广，甚至在今天的世界上仍有人效仿。“因此亲和数又有“相亲数”之称。

17世纪，法国的科坛上迸发出几束夺目的火花。1636年，“业余数学家之王”费尔马在致梅森的一封信中，毅然给出了第二对亲和数17296和18416。后来，梅森介绍了费尔马的求法：首先，列出算术数列2，4，8，…；将每一项乘以3，对应写在下方；将乘以3后得到的数列逐项减1，对应写在上方；最后，将乘以3后得到的数列逐项两两相乘后减1，即6·12－1，12·24－1，…，对应写在最下方。具体写法如下：

5	11	23	47	…
2	4	8	16	…
6	12	24	48	…
	71	287	1151	…

则当最下一行的某一项是素数时（如71），若它所在列的最上行的数字（如11）和它前面的数字（如5）也是素数，那么，71·4＝284，5·11·4＝220是一对亲和数。类似地，由1151·16＝18416，23·47·16＝17296，就得到了第二对亲和

数。

两年后，笛卡尔也写信告诉梅森，他得到了一个寻找亲和数的新方法：取2或2的任意次幂，把它乘以3减1（即$3\cdot2^n-1$）；再把它乘以6减1（即$6\cdot2^n-1$）；最后，即它的平方乘以18减1（即$18\cdot2^{2n}-1$）。若它们都是素数，则最后一项与2^n之积就是一对亲和数中的一个数。例如，$n=2$时，得284；$n=3$时，得18416；$n=6$时，就得到了第三对亲和数9437056及9363584。笛卡尔指出：费尔马的方法与他的方法是完全一致的。实质上，笛卡尔和费尔马的方法都符合于泰比特·依本克拉公式。或者说，他们各自独立地再次给出了泰比特·依本克拉公式。此后，人们按照这个公式验证下去，但是毫无结果。事实上，1891年勒拉瑟验证：当$n<35$时，只有$n=2$，4，7时可得到亲和数。1908年，杰热丁进一步证明：在$n\leqslant200$之内，只能得到上述三对亲和数。

在此过程中，还出现一些有趣的工作。例如，1652年，数学家斯库特恩给出一个用不定分析求亲和数的方法。即然考虑数对$4x$、$4yz$（x、y、z是奇素数），则$7+3x=4yz$，$y+7y+7z+3yz=4x$。消去x可得$z=3+16/(y-3)$。取$y=5$，得$z=11$，$x=71$，代入所设即得284和220。考虑数对$16x$，$16yz$，可得$z=15+256/(y-15)$。取$y=47$，即得第二对亲和数。考虑数对$128x$和$128yz$，可得$z=127+16384/(y-127)$。取$y=191$，可得到第三对亲和数。他还证明：不存在形如$2x$和$2yz$、$8x$和$8yz$、$32x$和$32yz$、$64x$和$64yz$的亲和数对。但是，斯特库恩并没能找到新的亲和数。事实上，在一百万之内，形如2^nx和2^nyz（x、y、z是奇素数，n是自数）的亲和数只有上述三对。

§2.2 欧拉的创举

18世纪，欧拉诞生在瑞士的国土上。他是一位数学奇才，正如法国物理学家阿拉哥所说："欧拉计算好象一点也不费力，正如人呼吸空气，或者老鹰乘风飞翔一样。"当然，亲和数也不会从他超人的思维中溜过。1747年，欧拉宣布：除了上述三对亲和数之外，他又找到了30对亲和数！就此一举引起数学界的轩然大波。由于欧拉仅列出了结果，没有证明，所以人们将信将疑。是啊！历代大师苦苦寻找了2000多年，才得到三对亲和数，而年仅39岁的欧拉竟一举给出了30对。3年后，欧拉给出了全部运算过程，并列出了一个包括64对亲和数的数表（其中有两对是错的），见表2·1。

下面，我们概括地介绍一下欧拉的方法，他是将亲和数划分为五种类型加以讨论的。

（1）寻找形如apq、ar的亲和数对，这里p、q、r是不能整除a的互异素数。欧拉分别讨论了$a=2^n$，$2^n f$（$f=2^{n+1}$+-是素数），$2^n(g-1)(h-1)$（后两个因数是素数）以及一些特殊值的情况，得到了第1、2、3、4、5、6、7、8、11、12、13对亲和数。

（2）寻找形如apq、ars的亲和数，这里p、q、r、s是不能整除a的互异素数。欧拉设$p=dx-1$，$q=\beta y-1$，$\gamma=\beta x-1$，$s=\alpha y-1$。当$\alpha=1$，$\beta=3$，$a=2^n$时，可得第α和第28对亲和数。当$\alpha=2$，$\beta=3$，$a=3^2\cdot5\cdot13$时，可得第32对。当$\alpha=1$，$\beta=4$，$a=3^3\cdot5$时，可得第30对。

（3）在（2）中，用一个数f（不一定是素数）替换s。

表2·1 **欧拉给出的亲和数表**

序号	m	n
1	$2^2\cdot71$	$2^2\cdot5\cdot11$
2	$2^4\cdot1151$	$2^4\cdot23\cdot47$
3	$2^7\cdot73727$	$2^7\cdot191\cdot383$
4	$2^2\cdot23\cdot827$	$2^2\cdot5\cdot137$
5	$3^2\cdot7\cdot13\cdot107$	$3^2\cdot5\cdot7\cdot13\cdot17$
6	$3^2\cdot5\cdot13\cdot289$	$3^2\cdot5\cdot11\cdot13\cdot19$
7	$3^2\cdot7^2\cdot13\cdot251$	$3^2\cdot7^2\cdot5\cdot13\cdot41$
8	$3^2\cdot5\cdot7\cdot102059$	$3^2\cdot5\cdot7\cdot53\cdot1889$
9	$2^2\cdot13\cdot17\cdot198899$	$2^2\cdot13\cdot17\cdot389\cdot509$
10	$3^2\cdot5\cdot19\cdot37\cdot7103$	$3^2\cdot5\cdot7\cdot19\cdot37\cdot887$
11	$3^4\cdot5\cdot11\cdot2699$	$3^4\cdot5\cdot11\cdot29\cdot89$
12	$3^2\cdot7^2\cdot11\cdot13\cdot19403$	$3^2\cdot7^2\cdot11\cdot13\cdot41\cdot461$
13	$3^2\cdot$[illegible]$\cdot13\cdot19\cdot17099$	$3^2\cdot5\cdot13\cdot19\cdot29\cdot569$
14	$3^2\cdot7^2\cdot13\cdot97\cdot11613$	$3^2\cdot7^2\cdot5\cdot13\cdot97\cdot193$
15	$3^2\cdot7\cdot13\cdot41\cdot163\cdot5867$	$3^2\cdot5\cdot7\cdot13\cdot41\cdot163\cdot977$
16	$2^3\cdot23\cdot59$	$2^3\cdot17\cdot79$
17	$2^4\cdot53\cdot607$	$2^4\cdot23\cdot1367$
18	$2^4\cdot5^3\cdot79$	$2^4\cdot47\cdot89$
19	$2^4\cdot89\cdot127$	$2^4\cdot23\cdot479$
20	$2^4\cdot103\cdot107$	$2^4\cdot23\cdot467$
21	$2^4\cdot239\cdot383$	$2^4\cdot17\cdot5119$
22	$2^4\cdot167\cdot1103$	$2^4\cdot17\cdot10303$
23	$2^4\cdot149\cdot191$	$2^4\cdot19\cdot1439$
24	$2^5\cdot79\cdot827$	$2^5\cdot59\cdot1103$
25	$2^5\cdot227\cdot2111$	$2^5\cdot37\cdot12671$
26	$2^5\cdot79\cdot7127$	$2^5\cdot53\cdot10559$
27	$2^6\cdot383\cdot2309$	$2^6\cdot79\cdot11087$
28	$2^8\cdot1151\cdot3067$	$2^8\cdot383\cdot9203$
29	$2^2\cdot11\cdot43\cdot107$	$2^2\cdot11\cdot17\cdot263$
30	$3^3\cdot5\cdot17\cdot31$	$3^3\cdot5\cdot7\cdot71$
31	$3^2\cdot5\cdot13\cdot29\cdot79$	$3^2\cdot5\cdot11\cdot13\cdot199$

32	$3^2\cdot5\cdot13\cdot29\cdot31$	3^2 $5\cdot13\cdot19\cdot47$
33	3 $\cdot5\cdot13\cdot19\cdot227\cdot263$	$3^2\cdot5\cdot13\cdot19$ $37\cdot1583$
34	3^2 $7^2\cdot13\cdot19\cdot89\cdot29399$	$3^2\cdot7^2\cdot11\cdot13\cdot19\cdot220499$
35	3^2 $5\cdot19\cdot37\cdot47$	$3^2\cdot5\cdot7\cdot19\cdot227$
36	$2^4\cdot67\cdot227\cdot401$	$2^4\cdot37\cdot67\cdot2411$
37	$3^2\cdot5\cdot31\cdot89$	$3^2\cdot5\cdot7\cdot11\cdot29$
38	$2\cdot5$ $23\cdot29\cdot673$	$2\cdot5\cdot7\cdot60659$
39	$2\cdot5$ $47\cdot359$	$2\cdot5\cdot7$ $19\cdot107$
40	$2^3\cdot31\cdot11807$	$2^3\cdot11\cdot163\cdot191$
41	$3^2\cdot7\cdot13$ $23\cdot79$ 1103	$3^2\cdot7\cdot13\cdot23\cdot11\cdot19\cdot367$
42	$3^3\cdot5\cdot23\cdot79\cdot1103$	$3^3\cdot5\cdot11\cdot19\cdot23\cdot367$
43	$2^3\cdot47\cdot2609$	$2^3\cdot11\cdot59\cdot173$
44	$2^3\cdot383\cdot1907$	$2^3\cdot11\cdot23\cdot2543$
45	$2^3\cdot467\cdot1151$	$2^3\cdot11\cdot23\cdot1871$
46	$2^3\cdot647\cdot719$	2^3 $11\cdot23\cdot1619$
47	$2^3\cdot191\cdot449$	$2^3\cdot11\cdot29\cdot239$
48	$2^3\cdot29\cdot47\cdot50$	$2^3\cdot17\cdot47\cdot93$
49	$2^4\cdot809\cdot51071$	$2^4\cdot17\cdot167\cdot13679$
50	$2^4\cdot1583\cdot7103$	$2^4\cdot23\cdot47\cdot9767$
51	$2^2\cdot43\cdot2267$	$2^2\cdot2\cdot13$ 1187
52	$3^2\cdot7.13\cdot131.971$	$3^2\cdot5\cdot7\cdot13\cdot17\cdot1187$
53	$3^5\cdot7^2\cdot13\cdot53.2543$	$3^5\cdot7^2\cdot11\cdot13\cdot53\cdot211$
54	$3^2.5^2\cdot17\cdot19.359$	$3^2\cdot5^2\cdot11\cdot59\cdot179$
55	$3^3\cdot5.17\cdot2^{7}\cdot397$	3^3 $5\cdot7\cdot21491$
56	$3^4\cdot7\cdot11^2\cdot19\cdot389\cdot863$	$3^4\cdot7\cdot11^2\cdot19\cdot47\cdot7019$
57	$3^4\cdot7\cdot11^2\cdot19\cdot179\cdot2087$	$3^4\cdot7\cdot11^2\cdot19\cdot53\cdot6959$
58	$3^5\cdot7^2\cdot13\cdot19\cdot389.863$	$3^5\cdot7^2\cdot13\cdot19\cdot47\cdot7019$
59	$3^5\cdot7^2\cdot13\cdot19\cdot179\cdot2087$	$3^5\cdot7^2\cdot13\cdot19\cdot53\cdot6958$
60	$2^5\cdot199$	$2^3\cdot19\cdot41$
61	$2^{[illegible]}\cdot19\cdot233$	$2^3\cdot41\cdot467$
α	$2^2\cdot17\cdot43$	$2^2\cdot5\cdot131$
β	$2^2\cdot13\cdot107$	$2^2\cdot5\cdot251$
γ	$2^4\cdot83\cdot2039$	$2^4\cdot19\cdot8563$

注 （1） 最后三个数对曾列于欧拉在1747年给出的30对亲和数之中。但是，不知为什么，在列此表时欧拉删去了它们。实际上，第α、第β对是对的，第γ对是错的。

（2）1915年，汝德指出：在这个表中，第34对和第γ对不是亲和数；第37对因印刷错误，将3^2误印为3^3。

则对于$a=4$，当$f=5$时，可求出第α与第β对亲和数；当$f=5\cdot13$时，可得第51对。对于$a=8$，当$f=17$时，可得第16对；当$f=11\cdot23$时，可得第44、45、46对。对于$a=16$，当$f=17$时，可得第21、22对；当$f=19$时可得第23对；当$f=23$时，可得第17、19、20对；当$f=47$时，可得第18对；当$f=17\cdot167$时，可得第49对。对于$a=3^3\cdot5$，当$f=7$时，可得第30对。

（4）寻找形如$agpq$、ahr的亲和数，这里p、q、r及g、h都是素数。设$g+1=km$，$h+1=kn$。对于$m=3$，$n=1$，当$a=10$，$k=8$，及$a=3^3\cdot5$，$k=8$时，可得第38、55对亲和数。

（5）寻找形如zap、zbq的亲和数，这里a和b是已知的，p和q是未知素数，而z是未知的但与a、b、p、q互素。当$a=5$，$b=1$时，可得第14、15对亲和数。继续改变a和b的值，又可得到9个新的亲和数对。

以上我们概述了欧拉的思想方法，他的每一个过程都是初等的，充分地显示出他超人的数学天才。他解开了令人止步2000多年的难题啊！因此，欧拉的工作曾使当时的数学家惊喜叫绝，无人与他争雄。可是，又过了100年，奇迹出现了。1866年，一位年仅16岁的孩子培格尼尼竟正确地指出：欧拉丢掉了第二对较小的亲和数1184和1210。这戏剧性的发现使数学家们如醉如痴，“亲和数啊，你这精灵！你怎么同数学大师开这样的玩笑？”不，中国有句古语，叫做智者千虑，必有

一失。况且科海苍茫，学无止境啊！这历史的妙趣，给人以何等深刻的启示！

1884年，西尔豪夫使用欧拉的方法，又得到了两对新的亲和数：$\begin{cases}3^2\cdot7^2\cdot13\cdot19\cdot23\cdot83\cdot1931\\3^2\cdot7^2\cdot13\cdot19\cdot23\cdot162287\end{cases}$ 与 $\begin{cases}2^6\cdot139\cdot863\\2^6\cdot167\cdot719\end{cases}$。

1911年，迪克森又给出两对亲和数：

$$\begin{cases}2^4\cdot12959\cdot50231 & 2^4\cdot10103\cdot735263\\ 2^4\cdot17\cdot137\cdot262079 & 2^4\cdot17\cdot137\cdot2990783\end{cases}$$

（与）。

1946年，电子计算机的产生，给亲和数的研究带来新的突破。用计算机寻找亲和数比较简单。它的基本方法是：对于每一个自然数n，先用机器确定它的所有因数（$\neq n$）及它们的和m；然后对m施行同样的运算，如果经过这一运算后回到原来的数n，那么就找到了一对亲和数（n，m）。例如，本世纪60年代，在美国耶鲁大学的计算机IBM7094上，对所有100万以下的数进行了清查，结果找到了42对亲和数，其中有一些是新发现的。例如，$3^3\cdot5\cdot7\cdot13$与$3\cdot5\cdot7\cdot139$，等等。计算机改变了人类对于计算能力的认识，机器以它单调、快速的运转向数学家们挑战！据本世纪70年代统计，人们已经找到了1200多对亲和数，一些运算程序甚至产生于中学生之手。面对此情此景，恐怕数学大师欧拉在九泉之下也会自愧不如了。截至1974年，人们已知的最大亲和数已达到152位数字，它们是

$$3^4\cdot5\cdot11\cdot5281^{19}\cdot29\cdot89\cdot(2\cdot1291\cdot5281^{19}-1)$$

$$3^4\cdot5\cdot11\cdot5281^{19}\cdot(2^3\cdot3^3\cdot5^2\cdot1291\cdot5281^{19}-1)。$$

§2.3 珠联璧合

尽管与完全数相比，亲和数的性质发现的不多。但是，仍然有一些值得描述的地方，现分述如下：

1. 性质

（1）任一素数都不会成为某一对亲和数中的一个数。

（2）若p^n是某一对亲和数中的一个数，则

$$\sigma(p^n)=\sigma\left(\frac{p^n-1}{p-1}\right)。$$

（3）1900年间，汉斯证明：若n和m是一对亲和数，则这两个数的全部因数的倒数之和的倒数和等于1。当$n=m$时，是完全数，这一性质与完全数的性质（7）相同（见§1.2）。

（4）由$\sigma(1+p)<1+p+p^2$可证：p^2绝不会是一对亲和数中的一个数。

（5）1908年，杰热丁证明：形如$2^2\cdot5x$、2^2yz的亲和数仅有欧拉表中的（α）、（β）；形如$2^4\cdot23x$、2^4yz的亲和数仅有（17）、（19）、（20）；形如$8xy$　$32z$的仅有(60)．这里x、y、z是奇素数。1911年，迪克森证明：在小于6233自然数中，只存在5对亲和数，即欧拉表中的（1）、（α）（β）、（60），和培格尼尼给出的一对。

2. 猜测

（1）人们观察到：当亲和数愈来愈大时，它们的比值

愈来愈接近于1。

（2）在已发现的亲和数对中，它们或者都是偶数，或者都是奇数。没有发现一个是奇数、一个是偶数的情况。本世纪60年代有人证明：对于$n \leqslant 3000\ 000\ 000$，没有发现一奇一偶的亲和数。

（3）1887年，卡特兰在研究完全数时认为：如果n_1是n的全部因数（不包括自身）之和，n_2是n_1的全部因数（不包括自身）之和，…，则$n, n_1, n_2, \cdots$有极限λ，这里λ是单位数或完全数。1888年，波热特指出：当$n=220$时，没有极限。因为$n_1=n_3=\cdots=284$，$n_2=n_4=\cdots=220$。1913年，迪克森指出：做适当的限定之后，这个猜测是成立的。

3．推广

（1）1902年，卡恩尼佛姆定义一种函数：$S^k(n)$。当$k=1$时，它表示n的全部因数（不包括自身）之和；当$k=2$时，它表示n的全部因数（不包括自身）和的全部因数（不包括自身）之和；……。显然，当n是完全数时，$S^k(n)=n$；当n、m是一对亲和数时，$s(n)=m$，$s^2(n)=n$。当$k>2$时，称n为联谊数，或k阶循环数。1913年迪克森指出：如果$n<6233$则不存在3、4、5、或6阶循环数。1918年，波里特给出一个5阶循环数$n=12496$，$S(n)=14288$，$S^2(n)=15472$，$S^3(n)=14536$，$S^4(n)=14264$，$S^5(n)=12496=n$。他还给出一个28阶循环数14316，它的循环过程如图2.1。表2.2中给出了这个28阶循环数的循环中各个数字的素因数分解。

表2.2　　一个28阶循环数表

第k阶数	第k阶时的数字	素因数分解	整除因数的个数
1	14316	$2^2 \cdot 3 \cdot 1193$	11
2	19116	$2^2 \cdot 3^4 \cdot 59$	29
3	31704	$2^3 \cdot 3 \cdot 1321$	15
4	47616	$2^9 \cdot 3 \cdot 31$	39
5	83328	$2^7 \cdot 3 \cdot 7 \cdot 31$	63
6	177792	$2^7 \cdot 3 \cdot 463$	31
7	295488	$2^6 \cdot 3^5 \cdot 19$	83
8	629072	$2^4 \cdot 39317$	9
9	589786	$2 \cdot 294893$	3
10	294896	$2^4 \cdot 7 \cdot 2633$	19
11	358336	$2^6 \cdot 11 \cdot 509$	27
12	418904	$2^3 \cdot 52363$	7
13	366556	$2^2 \cdot 91639$	5
14	274924	$2^2 \cdot 13 \cdot 17 \cdot 311$	23
15	275444	$2^2 \cdot 13 \cdot 5297$	11
16	243760	$2^4 \cdot 5 \cdot 11 \cdot 277$	39
17	376736	$2^5 \cdot 61 \cdot 193$	23
18	381028	$2^2 \cdot 95257$	5
19	285778	$2 \cdot 43 \cdot 3323$	7
20	152990	$2 \cdot 5 \cdot 15299$	7
21	122410	$2 \cdot 5 \cdot 12241$	7
22	97946	$2 \cdot 48973$	3
23	48976	$2^4 \cdot 3061$	9
24	45946	$2 \cdot 22973$	3
25	22976	$2^6 \cdot 359$	13
26	22744	$2^3 \cdot 2843$	7
27	19916	$2^2 \cdot 13 \cdot 383$	11
28	17716	$2^2 \cdot 43 \cdot 103$	11
29	14316	$2^2 \cdot 3 \cdot 1193$	11



图　2-1

（2）1636年，斯车恩特发现：27与35具有相同的因数之和（不包括自身）。1749年，克热福特认为45与3·29，39与55，93与145，45与13·19也具有这样的性质。1823年，泰勒把这种数称为不完全亲和数，并给出几对新的不完全亲和数：65与77，51与91，95与119，69与133，115与187，87与247。

（3）1913年，迪克森给出了三重亲和数的定义：它们每一个数的全部因数之和都等于其余两个数的和。例如，

$2^{14}\cdot3\cdot5\cdot19\cdot31\cdot89\cdot151$　　　$2^5\cdot3\cdot13\cdot293\cdot337$

$2^{14}\cdot5\cdot11\cdot19\cdot29\cdot31\cdot151$　　　$2^5\cdot3\cdot5\cdot13\cdot16561$

$2^{14}\cdot5\cdot19\cdot31\cdot151\cdot359$　　　$2^5\cdot3\cdot13\cdot99371$

就是两组三重亲和数，或称三联数。它们的关系如此吻合，难怪一些西方的数学家们爱昵地喻之为大仲马作品中的三个火枪手。

回顾数学家们寻找亲和数的漫长岁月，可能引起许多人的迷惘。人们会问他们终日兴致勃勃地玩弄那些枯燥的数字，目的何在呢？正如现代一位数学大师哈尔莫斯写道："甚至

受过教育的人们都不知我的学科存在，这使我感到伤心！

看来，数学家们寻觅知音的苦楚有胜于终日推演的艰辛。正如一首古诗表达的情怀：

一弹再三叹，慷慨有余音。

不惜歌者苦，但伤知音稀。

第三章 梅 森 数

探索者从希望开始。希望是探索者一直达到终点的理想阶梯。

——达 宁

§3.1 梅森数与梅森小史

所谓梅森数，是指形如2^n-1的数字，这里n是素数，当梅森数是素数时，就称之为梅森素数。例如，$n=2$时，$2^2-1=3$是第一个梅森素数；$n=3$时，$2^3-1=7$是第二个梅森素数，等等。当梅森数是合数时，就称之为梅森合数。例如，$n=11$（素数）时，$2^{11}-1=2047=23\cdot 89$是合数，因此，它就是一个梅森合数。

本世纪初，经美国数学家布勒提议，将这类数字冠以16世纪法国数学家梅森的名字。但是，它的研究却远远早于梅森时代，一直可以追溯到古希腊时期。

1．从欧几理得定理谈起

其实，了解完全数历史的人，对于梅森数就不会感到陌生。因为，在欧几里得给出的关于完全数的定理中，已经阐明了它与完全数的关系。即：当2^n-1是素数时，2^{n-1}（2^n-

1）是一个完全数。这就是说，每找到一个形如2^n-1的素数（即梅森素数），就会相应地产生一个完全数。我们知道：历代数学家都对完全数有着特殊的偏爱，它那完美的性质甚至使一些与数学不相干的人也很感兴趣（详见本书第一章完全数）。所以，几千年来，出于寻找完全数的需要，确定2^n-1是不是素数的工作，一直是数论研究的一大热门。

德国数学家高斯曾在《算术研究》一书中指出："把素数同合数鉴别开来，以及将合数分解成素因数的乘积，被认为是算术中最重要最有用的问题之一。"回顾梅森数的历史，它的研究正是从"鉴别素数"和"分解合数"这两方面展开的。

16世纪以前，人们寻找素数一般仅限于逐一试除法。即对于自然数n，设k是大于1、小于$\sqrt{n}$的自然数，则当k能被n整除时，n是合数；当k不能被n整除时，n是素数。古希腊时期，欧几里得首先指出，$n=2$、3时，2^n-1是素数。公元100年，尼可马修斯又给出了两对素数$2^5-1=31$和$2^7-1=127$。这些都是梅森数研究的先声。但是，随着指数n的增大，2^n-1的增长速度很快，所以在人们还没有发现判定素数的新方法之前，这一工作的进展十分缓慢，直到1456年，才有人给出了第五个素数$2^{13}-1=8201$。

16世纪、许多人曾围绕着2^9-1和$2^{11}-1$是素数还是合数的问题，展开了激热争论。鲍威鲁斯，热契和斯蒂佛尔等人，都在著作中把它们列为素数，并且几乎得到了数学界的公认。1536年，数学家热格斯力排众议，明确指出：这两个数都是合数，它们的因数分解是$2^9-1=7\cdot73$，$2^{11}-1=23\cdot89$。今天看来，这个问题太简单了，即使是中学生也会毫不费力地

解决它们。例如，$2^9-1=(2^3)^3-1=(2^3-1)(2^6+2^3+1)=7\cdot73$，多么简明的因式分解！然而在16世纪，却引起数学界的众说纷纭。

1603年，克特迪正确指出：$2^{13}-1$、$2^{17}-1$和$2^{19}-1$是素数。至此，人们已经确定了七个梅森素数和一个梅森合数。在这一过程中，人们还没有很好地研究2^n-1的数学性质，只是在一般的验证中探索。因此，可以说：16世纪以前是梅森数研究的初级阶段，它是与完全数研究并行的。

2．名字的由来

1588年9月8日，马林·梅森出生在法国奥泽附近。早年，他就学于欧洲著名的拉·弗来施公学，后来，迫于社会习俗的压力，进入一座小修道院，成为终身神甫。

在17世纪的欧洲，梅森是数学界一位独特的中心人物。他学识广博，才华横溢，并且是笛卡尔、费尔马、惠更斯、帕斯卡等许多大科学家的密友。从完全数和亲和数的研究中，我们已经看到：许多科学家每获得一项科学发现，都乐于将成果寄给梅森，然后由梅森转告给更多的人。出现这一现象的原因不仅在于他们的友情，还有一个重要的历史因素，就是当时的欧洲，科学刊物和国际会议等学术活动还远远没有产生，甚至连科研机构都没有创立。所以，科学研究的交流是十分困难的。在这种情况下，梅森凭借自己广泛的交往和热情诚挚的为人，自然起到了科学交流的桥梁作用。

后人从梅森的往来信件和科研总结中看到：他对于2^n-1形数字的记载翔实而丰富。并且，同费尔马、笛卡尔等人进行过多次的争论和研究，其中有许多惊人的灼见。1640年6月，费尔马在致梅森的一封信中写道："在艰深的数论研究

中，我发现了三个非常重要的性质。我自信：它们将成为今后解决素数问题的基础。” 现将这三个性质叙述如下：

定理（费尔马） （1）如果n是合数，则2^n-1是合数。

（2）如果n是素数，则$2n|2^n-2$。

（3）如果n是素数，2^n-1是合数，则2^n-1只能被形如$2kn+1$的素数整除，其中k是某个正整数。

证明 （1）分两种情况：①若n是偶合数，不妨设$n=2x$其中x是大于1的正整数。则有$2^n-1=2^{2x}-1=(2^x-1)(2^x+1)$，显然是合数。②若$n$是奇合数，则它必能分解成两个或两个以上的因数之积，设$n=pq$，其中p、q是大于1的正整数。则有$2^n-1=2^{pq}-1=(2^p-1)[(2^p)^{q-1}+(2^p)^{q-2}+\cdots+(2^p)+1]$。因为$1<p<n$，所以$1<2^p-1<2^n-1$，即$2^p-1$是$2^n-1$的真因数*。所以$2^n-1$是合数。综合①、②，（1）得证。

（2）这是费尔马小定理的一种特殊情况，我们将在本书第六章中详细介绍。此处证明略。

（3）设$q>1$是2^n-1的一个素因数，则有$q|2^n-1$。又根据本地理(2)可推知$q|2^{q-1}-1$。因为2^n-1与$2^{q-1}-1$的最大公因数***等于2^g-1，其中g是n与$q-1$的最大公因数**，即$g=(n,q-1)$，所以可证：$g>1$。假设不成立，即$g=1$，则$(2^n-1, 2^{q-1}-1)=2^1-1=1$。但是，由上述知$q|2^n-1$，且$q|2^{q-1}-1$，$q>1$，矛盾，因此$g=1$不成立，只有$g>$

---

* 若$a=bc$，而b既不等于a又不等于1，则称b是a的真因数。

** 如果$c|a$且$c|b$，则c叫做a和b的公因数；如果c是a和b的公因数中最大的一个，则c叫做a和b的最大公因数，记作$(a, b)=c$。

*** 这一结论引用了一个定理：如果a、b和s是正整数，则如果$(a, b)=g$，那么$(s^a-1, s^b-1)=s^g-1$。证明略。

1。从而知n与$q-1$不互素。又因为n是素数，所以只有$n|q-1$，即$q-1=mn$，其中m是某正整数，或表为$q=mn+1$。若m是奇数，又知n是奇素数，则$q=mn+1$将是偶数，因此而不是素数，矛盾。所以m必是偶数，设$m=2k$，k是某正整数，代入得$q=2kn+1$。由q的任意性，（3）得证。

注 对于这三个性质，当时费尔马只提出来了，并没有证明。它们的证明是1747年由欧拉完成的。

费尔马的工作改变了人们盲目探索的局面，大大紧缩了确定素数的验证范围。梅森正是以此作为思想基础展开工作的。他在短短的四年间，检验了直至$2^{257}-1$的全部数字，并且于1644年，在他的《思考》一书中写道："总结前人的工作和我个人的研究，可以得到结论，在小于或等于257的数字中，仅当$n=2$，3，5，7，13，17，19，31，67，127和257时，2^n-1是素数；对于$n<257$的其它数值，2^n-1都是合数。"对于这一论断，梅森曾陆续给出一些不完善的解释。但是，4年后他离开了人世，终止了计算。

事实上，梅森的证明中包含着许多错误和不足，对此我们将在后文详述。但是，由于他科学地总结了前人的成果，首先将费尔马的思想付诸实践，可以说，梅森的工作是素数研究的一个转折点和里程碑。因此，将形如2^n-1（n是素数）的数字冠以他的名字是毫不过分的。另外，数论中通常将这类数字记作M_p，其中M是梅森原名Mersenne的第一个字母，p是2^p-1的素指数。

§3.2 素数之最

为了叙述方便，我们将梅森素数与梅森合数的研究分开

来介绍。本节内容仅涉及梅森素数的有关问题。

在梅森的那段话中，前半部分，即"$p=2$，3，5，7，13 17，19时，2^p-1是素数"这一结论，是他整理前人的工作得到的，它们的正确性已经被证实。而属于"猜测"内容的只有$n=31$，67，127，257。这几个数比较庞大，其中最小的$2^{31}-1=2147483647$，也具有10位数字。可以想象，它们的证明是十分艰巨的。正如梅森推测："一个人，使用一般的验证方法，要检验一个15位或20位的数字是否为素数，即使用终生的时间也是不够的。"是啊，枯燥、冗长的运算会耗尽一个人的毕生精力，谁愿意让生命的风帆永远在黑暗中颠簸！看来，伟人的"猜测"只有等待后来的伟人来解决了。

1. 欧拉及$2^{31}-1$

果然，约100年后，这个问题落到了欧拉的手上。于是，素数的数学生命复活了。1747年，欧拉首先完成了上述定理（费尔马）的证明。接着，他又卓越地发展了费尔马的思想，提出一个更有趣的定理。

定理（欧拉） 对于素数$p>2$，2^p-1的每一个素因数必具有$8k\pm1$的形式。

略证 设$q=2Q+1$是2^p-1的一个素因数，则$q|2(2^p-1)=2^{p+1}-2=N^2-2$，其中$N=2^{(p+1)/2}$。因此$2=N^2-k_1q$，$k_1$是某正整数。进而可推得$2^Q=N^{2Q}-k_Qq\cdots(1)$，$k_Q$是某正整数。由于$q\nmid2$，知$q\nmid N$，所以由费尔马小定理（见第六章）有$q|N^{2Q}-1$。再根据(1)式得$q|2^Q-1$。从而，根据数论中的另一条定理*可知$q=8k\pm1$，$k$是某正整数。

---

* 这一定理是：若$q=2Q+1$是素数，则：如果$q|2^Q-1$，必有$q=8k\pm1$，如果$q|2^Q+1$，必有$q=8k\pm3$。此定理的证明较繁，故略去。

欧拉的这一发现，进一步紧缩了梅森数的确定范围。不过，这仅仅是理论上的突破．在很长一段时间里，欧拉并没有对“梅森猜测”给出任何说明。因为这种说明单凭论证技巧是不够的，它需要大量繁重的计算！正如一位数学家所说，数学研究具有两个重要途径：证明和计算。它们的区别在于，计算是容易、繁杂、枯燥、刻板的，而证明却是困难、简练、美妙、灵活的。欧拉可以在理论证明中充分发挥他的才智，做出伟大的工作。但是，在计算面前，却人人平等。即使有超人的才华，也非花费大气力不可。

应该承认，欧拉是数学领域中的强者。在他的手下，众多的数学难题都突破了．在梅森数面前他也不会止步。1772年，欧拉已双目失明。但是，他用心算再度向梅森数冲击。有一天，他终于兴奋地转告另一位数学伟人贝努利：“我已经严格地证明了，$2^{31}-1$确是一个素数”。回顾欧拉的推演过程，有许多独到的见解．他那纯熟的运算技巧实在令人叹为观止．现将他的方法概述如下：

因为$\sqrt{2^{31}-1}=\sqrt{2147483647}\approx 46340$．所以只须用$<46340$的素数试除$2^{31}-1$。又根据费尔马和欧拉分别给出的定理，若$2^{31}-1$有真因数，它必具有$2pk+1=2\cdot 31\cdot k+1=62k+1$的形式；并且具有$8k\pm 1$的形式。设$k=4j+m$，这里$m=0$，1，2，3，则形如$62k+1$的素数只有四种类型：

$$248j+1=8(31j)+1,$$

$$248j+63=8(31j+8)-1,$$

$$248j+125=8(31j+16)-3,$$

$$248j+187=8(31j+23)+3.$$

显然，具有$8k\pm 1$形式的只有前两式，因此可将后两式排除。

总结上述证明可知，若$2^{31}-1$存在真因数q，则必满足$q<46340$，且$q=248k+1$或$q=248k+63$。在此限定下，欧拉进行了大量的验算，(一共试除了84个因数)，最后证明，这样的真因数q是不存在的，所以$2^{31}-1$是素数。

欧拉是在双目失明的情况下完成上述工作的。这是多么顽强的毅力！难怪大数学家拉普拉斯向他的学生们说："读读欧拉，读读欧拉，他是我们一切人的老师。"

2．鲁卡斯等人的工作

欧拉的艰辛给人们提示：在伟人难以突破的困惑面前要想确定更大的梅森素数，只有另辟蹊径了。

100年后，法国数论家鲁卡斯在研究著名的斐波那契数列时，竟惊人地发现了它与梅森数的渊源。所谓斐波那契数列'是指：

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ \cdots,$$

它的通项公式是：$u_1=u_2=1$，$u_{n+1}=u_{n-1}+u_n\ (n>1)$。这个貌似平凡的数列，在数学中占有非常重要的地位(详见本书第四章斐波那契数列)。1876年，鲁卡斯发展了斐波那契的递归思想，将这一数列推广。他的基本方法是：

设$v_1=1$，$v_2=3$，$v_{n+1}=v_{n-1}+v_n$，则

$$v_n=\left(\frac{1+\sqrt{5}}{2}\right)^n+\left(\frac{1-\sqrt{5}}{2}\right)^n=\frac{u_{2n}}{u_n},$$

其中 $$u_n=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

这个式子是斐波那契数列通项的一种表示法，即比内公式。它在数学中非常著名。

鲁卡斯又设$R_n=v_{2^n}$，则可以得到数列：

3，7，47，…，

它的通项公式是$R_1=3$，$R_{n+1}=R_n^2-2$。利用这个数列，鲁卡斯给出一个非常有趣的定理。

定理（鲁卡斯） 如果$4|p-3$，其中p是素数，则当且仅当M_p是素数时，$M_p|R_{p-1}$。

例如，当$p=7$时，显然$4|(7-3)$，而$R_1=3$，$R_2=7$ $R_3=47$，$R_4=2207$，$R_5=4870847$，$R_6=23725150497407$·可以验证：$2^7-1|R_6$，所以$M_7=2^7-1$是素数。

鲁卡斯定理具有十分重要的意义，它改变了梅森数在数学中的“附属”地位，使之成为人们寻找已知的“最大素数”的热点。我们知道，欧几里得曾证明：素数是无限多的。而在无限多的素数中，寻找已知的最大素数，一直是数论研究的一项重要工作。从鲁卡斯时代起，梅森素数就变成了“素数之最”，这一优势一直延续至今。

在给出上述定理之后，鲁卡斯首先证明了：$M_{127}=2^{127}-1=170141183460469231731687303715884105727$是一个素数。它具有39位数字，早在17世纪，梅森就认为它是素数（见§3.1），但无力证明。是鲁卡斯的工作使它由“猜测”变成事实。M_{127}还是电子计算机产生之前，人们用手算得到的最大素数。

不过，鲁卡斯定理有一个致命的弱点，就是它的约束条件$4|p-1$使之仅适于验证一部分梅森数。例如，在梅森猜测中，包括$M_{61}=2^{61}-1$，$M_{257}=2^{257}-1$，由于$4\nmid(61-3)$，并且$4\nmid(257-3)$，不符合定理条件，所以无法验证M_{61}和M_{257}是否为素数。为了消除这一弱点，鲁卡斯改变了定理的初值，给出一个更为出色的定理。

定理（鲁卡斯法则） 梅森数$M_p>3$是素数的充分必要条件是$M_p|S_{p-1}$，这里$S_1=4$，$S_2=14$，$S_{n+1}=S_n^2-2$。

这一定理适用于大于3的全部梅森数。例如，$M_5=2^5-1=31$。由于$S_1=4$，$S_2=14$，$S_3=194$，$S_4=37634$，而且$M_5|S_4$，所以M_5是一个素数。鲁卡斯的工作再次给梅森数的研究带来生机。1883年，波佛辛首先证明$M_{61}=2^{61}-1$是一个素数；1886年，赛尔豪夫再次证明这一结论；1887年，哈德劳特以54小时作为代价，又一次验证了M_{61}是素数。

人们大概觉得，这一工作仍然如此费力！其实与老办法相比，它已经有了极大的改观。如果我们使用16世纪克特迪（他曾证明M_{19}是一个素数）的方法，即用小于$\sqrt{M_{61}}\approx1.5\times10^9$的数试除$M_{61}$，这样的数有$75\times10^6$个，因此要试除7000多万次！如果我们使用17世纪费尔马的方法，即假设M_{61}有素因数，必是$2\times61\times k+1=122k+1$形式的数，其中$k$是正整数。需要对$M_{61}$进行试除的这类数字有$1.25\times10^6$个，因此要试除1000多万次！如果我们根据18世纪欧拉的方法，即假设M_{61}有素因数，必是$488k+1$或$488k+367$的形式，其中k是正整数。需要对M_{61}进行试除的这类数字有0.62×10^6个，因此要试除60多万次！但是，波佛辛等人使用的鲁卡斯法则验证M_{61}的性质，仅需要乘法60次，减法60次，除法60次，即180次运算。克特迪等人的方法与此相比，真可谓"小巫见大巫"了。实际上用鲁卡斯法则检验M_{61}所需要的时间，仅相当于欧拉方法检验M_{31}或卡特迪方法检验M_{19}所需要的时间。

1911年，鲍尔等人在确定梅森合数的因数时，意外地发现：$M_{89}=2^{89}-1$也是一个素数！这是被梅森遗漏掉的。它

提示人们：不能盲目地相信古人，只能相信事实。果然在1914年，鲍尔再次发现了梅森的失误：$2^{107}-1$也是一个素数。

应当指出：在鲁卡斯法则中，数列$\{S_n\}$的增长速度极快。例如，$S_4=37634$已是5位数字，要想检验M_{61}，就要求出S_{60}，这种运算量是惊人的。所以，随着数字的增长，如何改进鲁卡斯法则是非常重要的。1930年，美国加利弗尼亚大学的D·H·莱赫默教授修正了鲁卡斯的工作，给出了一个新的判别法。

定理（鲁卡斯－莱赫默） 梅森数$M_p>3$是素数的充分必要条件是$S_{p-1}=0$。其中$S_1=4$，$S_{n+1}=S_n^2-2 \bmod M_p$*。

莱赫默工作的最大效应是避免了S_n增长过快，但增加了运算次数。例如，验证2^7-1是素数。考虑数列：

第一项是4，

第二项是$4^2-2=14$，

第三项是$14^2-2=194$，

因为$194>127$，所以用194除以127，余67，则有：

第四项是$67^2-2=4487$，用127除，余42，

第五项是$42^2-2=1762$，用127除，余111，

第六项是$111^2-2=12321$，用127除，余0。

所以，M_7是一个素数。

3．计算机时代

在电子计算机产生之前的2000多年间，人们历尽艰辛，仅找到了12个梅森素数。它的主要障碍就是繁冗的数字运

---

* 这是同余符号，即$a\equiv b \bmod m$，当且仅当$m\mid(b-a)$。

算。鲁卡斯等人的方法虽然有许多优点，但是莱赫默曾证明，当p增大时，它的计算次数大约和p的立方成正比。就是说，测试M_{2r+1}所需要的时间，将是测试M_r所需时间的8倍！因此，如何有效地缩短运算时间，已成为问题的症结！

1946年，电子计算机的产生改变了人们对于自身运算能力的认识，它使许多过去“不可能”的事情成为现实。尤其是计算机的工作原理非常适用于数字运算，所以在它诞生不久，就在“判定素数”中产生了效应。最早的突破是1952年初，英国剑桥大学的学者们使用EDSAC计算机，求出了一个具有79位数字的素数：

$$180(2^{127}-1)^2+1。$$

这个数字似乎与鲁卡斯确定的素数$M_{127}=2^{127}-1$有些关系，它首次达到了梅森素数在“最大素数中的领先地位。”

但是，这种突破十分短暂。同年，美国加利福尼亚大学的计算机SWAC开始工作。数学家鲁宾逊等人成功地将鲁卡斯-莱赫默方法编译成计算机程序，输入SWAC。在短短的几小时之内，他们检验了42个梅森数，其中最小的也有80位数字。最后证明：在$127<p<2309$之间，只存在5个梅森素数，它们是M_{521}，M_{607}，M_{1279}，M_{2203}，M_{2281}，其中最小的M_{521}竟是157位的巨数。与手算相比，SWAC计算机的效率是惊人的。例如，它在检验$M_{1279}=2^{1279}-1$（具有386位数字）时，仅用了13分30秒钟。如果一个人用手算，则至少需要25年！

1957年，黎塞尔使用瑞士的斯韦迪士计算机BESK证明：在$2300<p<3300$之间，仅有一个梅森素数M_{3217}，它有969位数字，是第18个梅森素数。

注 顺便说明一下：对于一个巨大的梅森数，要想确定它的位数，用不着真正地去计算这个数，而可以利用对数方法。即

对于$M_p=2_p-1$，先求$M_p+1=2^p$的位数。因为$\lg 2^p=p\cdot\lg 2=p\times 0.30103$，所以$M_p+1$的位数就等于$p\times 0.30103$的整数部分再加1。例如，$M_{3217}+1=2^{3217}$，从而$p\times 0.30103=968.414\cdots$，所以$M_{3217}+1$的位数是969。还可以证明：$M_p$与$M_p+1$有相同的位数。因为，假设$M_p+1$多一位数，那么它的末位必为0，但这对于2的任意次幂是不可能的。2^p的末位数只能是2，4，6，8，这一点不难证明。

1961年，赫维兹使用一台IBM7090电子计算机证明：在$3300<p<5000$之间，只有两个梅森素数M_{4253}、M_{4423}。在检验M_{4423}时，IBM7090使用鲁卡斯-莱赫默方法，花费了大约50分钟。此后人们试问：在$5000<p<50000$之间，有多少个梅森素数呢？萨克斯利用素数分布理论证明：对于$p_n\leqslant P\leqslant P_m$之间，梅森素数$M_p$约有

$$P=\frac{1}{\lg 2}\sum_{p_n}^{p_m}\frac{1}{p}\text{（个）}.^{*}$$

由此推测：在$5000<p<50000$之间，约有5个梅森素数**。

1964年，伊利诺斯大学的吉里斯教授证明：当$p=9689$，6941，11213时，M_p也是素数。其中M_{11213}具有3376位数字，该校数学系为纪念这一伟举，在它寄出的每一封信上都印了这个数字，即$2^{11213}-1$。吉里斯还猜测：当p在x与$2x$之间时，约给出两个梅森素数，其中x是大于1的正整数，例如，$x=2$时，$2x=4$，显然，$p=2$，3使M_2、M_3是素数。他

---

* Σ是求和符号。例如，$\sum_{i=1}^{n} i=+12+\cdots+n$。

** 直至1979年才证实：在$500<p<5000$。之间，存在7个梅森素数。

的猜测与现在已知的结果相符。另一位数学家厄伯哈特则猜测：第n个梅森素数的p值大约是1.5的n次方。例如，$(1.5)^{23} \approx 11223$，实际上第23个梅森素数是M_{11213}，p值非常接近！

吉里斯之后，人们好多年没有找到更大的梅森素数。直至1971年3月4日晚上，塔克曼郑重宣布：又一个新的梅森素数诞生了，它是M_{19937}，具有6002位数字。若将$2^{19937}-1$展开写，将占满本书约整整八页！面对如此巨数，人类的计算能力再度陷入困境。此时，能否找到更大的梅森素数，将包括两种含义：一是在数学中提出新的检验方法，再一是制造出运算更快的计算机。所以，近年来对于梅森素数的研究能力如何，在某种意义上将标志着一个国家的科学水平！

1978年10月，两位年仅18岁的美国大学生诺尔和尼可打破了人们长时间的沉默．他们宣布：找到了第25个梅森素数M_{21701}。当时，美国所有的大新闻通讯社都报道了这个消息，甚至电视台上最有名的新闻报道人克朗凯，也在哥伦比亚广播公司的晚间新闻节目中宣布了这个消息。

翌年2月，美国另一位数学家史洛温斯基，利用本研究所中的克雷一号计算机开始寻找梅森素数。这是一种超高速计算机．例如，1953年，韦勒用伊利亚克一号检验M_{8191}（这个数字，我们将在下一节提到）时，花费100小时；若是赫维兹使用的IBM7090，需要5.2小时；伊利亚克二号需要49分钟；IBM360/91需要3.17分钟；而用克雷一号只需要10秒钟！

注　克雷一号（原名Cray-I）是亿次巨型计算机，相当于我国自行制造的亿次巨型银河计算机。

1979年2月23日，史洛温斯基克服困难，终于找到了第26个梅森素数M_{23209}，正当他欢喜若狂之际，有人冷静地告诉他："诺尔先生已在两星期之前得到了同样的结果。"当时，诺尔使用塞伯174计算机花费了8小时40分钟，而克雷一号只花费了不到7分钟！由此，史洛温斯基潜心发愤，努力向第27个梅森素数进攻。但是，根据厄伯哈特的猜测，因为$(1.5)^{27}\approx 57000$，所以第27个梅森素数M_p的指数p将是接近5万的大数。按照已有的方法，克雷一号要花费2000小时！为了缩短时间，史洛温斯基改进了计算机程序，大大简化了运算，在试了约1000个数之后，终于在同年4月3日找到了第27个梅森素数M_{44497}，他花费了300小时！同时还证明：在$p<50000$中，再没有其它梅森素数。

1983年，史洛温斯基等人利用克雷一号进一步证明：在小于2^{62982}的范围内，只有27个梅森素数。同年10月，他们越过2^{62982}，从$p=75000$一直计算到$p=100000$，结果又找到一个梅森素数M_{86243}。年末，又找到M_{132049}。1985年，他们再接再励，又找到了M_{216091}。这最后一个数具有65050位数字，展开写可以占满本书约100页！但是，史洛温斯基并不知道在2^{62982}与2^{75000}之间，以及在$2^{132049}-1$与$2^{216091}-1$之间是否还有其它的梅森素数，因此也就无法确定这三个巨数处于梅森素数中的第n位！见梅森素数一览表

§3.3 "合数之最"

一般说来，合数研究主要包括两个基本内容：一是确定它是否为合数，再一是找到它的全部素因数。根据基本分解

表3·1　　梅森素数表

序号	2^p-1	位数	发现年代	发现者
1	2^2-1	<1	约公元前300年	欧几里得
2	2^3-1	<1	约公元前300年	欧几里得
3	2^5-1	<2	公元100年	尼可马修斯
4	2^7-1	<3	公元100年	尼可马修斯
5	$2^{13}-1$	4	1456年	无名氏
6	$2^{17}-1$	6	1603年	克特迪
7	$2^{19}-1$	6	1603年	克特迪
8	$2^{31}-1$	10	1772年	欧拉
9	$2^{61}-1$	19	1883年	波佛辛
10	$2^{89}-1$	27	1911年	鲍尔
11	$2^{107}-1$	33	1914年	鲍尔
12	$2^{127}-1$	39	1876年	鲁卡斯
13	$2^{521}-1$	157	1952年	鲁宾逊
14	$2^{607}-1$	183	1952年	鲁宾逊
15	$2^{1279}-1$	386	1952年	鲁宾逊
16	$2^{2203}-1$	664	1952年	鲁宾逊
17	$2^{2281}-1$	687	1952年	鲁宾逊
18	$2^{3217}-1$	969	1957年	黎塞尔
19	$2^{4253}-1$	1281	1961年	赫维兹
20	$2^{4423}-1$	1332	1961年	赫维兹
21	$2^{9689}-1$	2917	1964年	吉里斯
22	$2^{9941}-1$	2993	1964年	吉里斯
23	$2^{11213}-1$	3376	1964年	吉里斯
24	$2^{19937}-1$	6002	1971年	塔克曼
25	$2^{21701}-1$	6533	1978年	诺尔
26	$2^{23209}-1$	6987	1979年2月	诺尔
27	$2^{44497}-1$	13395	1979年4月	史洛温斯基
28?	$2^{86243}-1$	25960	1983年10月	史洛温斯基
29?	$2^{132049}-1$	39751	1983—1984年初	史洛温斯基
30?	$2^{216091}-1$	65050	1985年	史洛温斯基

定理：

每一个大于1的正整数或者是素数，或者是若干个素数的乘积。并且，一个数的素因数分解式是唯一的。

例如，72是一个合数，而$72=2^3\cdot3^2$是它唯一的素因数分解式。

梅森合数的历史并不久远，它始于16世纪。在此之前人们曾认为：只要p是素数，则2^p-1就是一个素数。例如，当$p=2$，3，5，7时，2^p-1都是素数。但是，1536年，数学家热格斯发现，当$p=11$（素数）时，$2^{11}-1=2047=23\cdot89$是一个合数，从而否定了前人的猜想，开创了所谓“梅森合数”的研究。

1. 因数分解

梅森合数常常是梅森素数研究的“副产品”。并且，它们大都产生于数学家的错误猜测之中。例如，1603年，卡特迪认为，当$p=23$，29和37时，2^p-1是素数。但是，1640年，费尔马在给出关于梅森数的定理（见§3.1）的同时，还告诉梅森：$2^{37}-1$不是素数，它有因数223。同年11月他又告诉福兰尼克：$2^{23}-1$也不是素数，它有因数47。从而部分地否定了卡特迪的论断。费尔马成功的原因是发现了“如果2^p-1是合数（p是素数），则它的真因数必形如$2pk+1$”这一定理，从而大大削减了运算量。例如，$2^{23}-1=8388607$，为找到它的因数，只须用形如$2\cdot23k+1=46k+1$（其中k是正整数）的数验证，即取$k=1$，2，3……等值，试除$2^{23}-1$就可以了。$k=1$时，$46k+1=47$。而$47\mid2^{23}-1$，因此找到了$2^{23}-1$的一个真因数。这显然要比盲目试除简单得多。1732年欧拉证明：$2^{29}-1$也不是素数，它有因数1103。他的成功也

是利用了费尔马的方法。

应当指出，费尔马方法仅是关于梅森合数的一个必要条件。就是说：虽然梅森数M_p的因数必为$2pk+1$的形式，但是形如$2pk+1$的数不一定是2^p-1的因数。17世纪，人们并没有清楚地认识到这一点，例如，1678年庞利就认为$2^{41}-1$可以被83整除，因为$83=2\cdot41-1$。这是一个错误。

1738年，欧拉给出一个定理，现叙述如下：

定理（欧拉） 如果$4m-1$和$8m-1$是素数，其中m是正整数，则$8m-1$整除$2^{4m-1}-1$。例如：当$m=3$时，$4m-1=11$是素数，$8m-1=23$也是素数，显然有$23|2^{11}-1$。欧拉根据这条定理证明了：当$p=83$，131，179，191，239时，2^p-1是合数，它们分别具有形如$8m-1$的因数167，263，359，383，479。同时，欧拉还证明：当$p=43$和73时，2^p-1也是合数，它们分别有因数431和439。上述成果再度显示出欧拉超人的天赋。但是，他也有失误之处，那就是他错误地认为$2^{41}-1$和$2^{47}-1$也是素数。

1856年，热斯切尔找到了$2^{47}-1$的两个因数2351和4513他还证明：当$p=233$，79，113，179，239时，2^p-1分别有真因数1399，2687，3391，1433，1913。1859年，蒲拉那严格地得到了M_{41}的因数分解（它只有两个素因数）：

$$2^{41}-1=13367\times164511353。$$

他还指出，$2^{53}-1$也是合数，并且错误地预测它没有小于50033的因数。1869年，兰德给出下面四个数完整的因数分解：

$$2^{43}-1=431\cdot9719\cdot2099863，$$

$$2^{47}-1=2351\cdot4513\cdot13264529$$

$$2^{53}-1=6361\cdot69431\cdot20394401,$$

$$2^{59}-1=179951\cdot3203431780337.$$

显然，他否定了蒲拉那关于M_{53}因数位数的猜测。并且，给出一个新的梅森合数M_{59}。

1877年，鲁卡斯运用费尔马小定理（见本书第六章伪素数）证明了上述欧拉给出的定理。他的基本方法是：因为$8m-1$是素数，且$(2, 8m-1)=1$，所以由费尔马小定理有$8m-1\mid2^{8m-2}-1=(2^{4m-1+1})(2^{4m-1}+1)$。又根据$4m-1$是素数可证$8m-1\mid2^{4m-1}-1$。利用这一定理，鲁卡斯进一步证明：当$p=251$，359，419，431，443，491时，$2^p-1$也是合数。其中$2^{251}-1$是“梅森猜测”中的最后一个合数，人们已找到它的两个因数503和54217，但是其它的素因数还没有找到。

1878～1882年间，勒拉舍证明：当$p=97$，211，151，223时，2^p-1分别有因数11447，15193，18121，18287。他还认为：当$p=61$，67，71，89，101，103，107，109，127，137，139，149，157，163，167，173，181，193，197，199，227，229，241，257时，2^p-1不存在小于30000的因数。这个论点包含了一些错误，例如，1894年库尼佛姆找到了$2^{197}-1$的一个因数7487，它显然小于30000。库尼佛姆还进一步指出：在勒拉舍的数表中，除掉$p=61$和197之外，其它的2^p-1不存在小于50000的因数。其实他的论点也不准确，1910年伍德奥尔证明$2^{181}-1$有因数43441，它小于50000！

回顾梅森数因数分解的历史，读者可能觉得平淡无奇。实际上这里面蕴含着历代数学家无比艰苦的工作，有些结果甚至经过数年的努力才产生的。一个有趣的故事足以说明这

一点。1903年，在美国的一次数学会议上，一位名叫科尔的数学教授默默地走上讲台，他在黑板上写出两个大素数：193707721和761838257287，将它们相乘，得到积数；然后，他又将$2^{67}-1$展开，其结果与上面两个大素数的乘积完全相同。这时，科尔放下粉笔，又默默地走回了座位。会场沉默片刻之后，顿时爆发出热烈的掌声。原来，这场“无声的讲演”告诉人们：科尔已完成了$2^{67}-1$的因数分解！这是300年前“梅森猜测”中的一个难题，当时梅森曾认为它是素数；1876年鲁卡斯证明了它是合数，但无力找出它的因数。是科尔教授完成了这项艰巨的工作。当人们询问他花费了多少时间时，科尔静静地说：“三年内的全部星期天！”

2．梅森合数表

到目前为止，人们已经确定了许多梅森合数。它们大体上可以分为三类：第一类是已经找到了完整的因数分解式；第二类是找到了它们的部分因数；第三类是仅知道它是合数，却找不到它的因数。限于篇幅，本书不能一一列出每个梅森数的研究过程。为了便于查阅，现列出一个指数p小于257的梅森合数表，以期达到“管中窥豹”的效果，需要说明一下，我们之所以取257作为列表的上限，是因为三百多年前“梅森猜测”就以此作为上限。

还有一个值得提及的大合数M_{8191}。1876年卡特兰根据已知的结果推测：当p是梅森素数时，M_p也一定是梅森素数。例如，$M_2=3$，$M_3=7$，$M_5=31$，$M_7=127$是素数，而以它们作为指数p，得到的M_3、M_7、M_{31}和M_{127}也是素数。下一个梅森素数是$M_{13}=8191$，所以人们推测M_{8191}也是素数。直至1953年，韦勒使用ILLIAC计算机花费100小时证明：

表3·2 $P<257$的梅森合数(M_p)表

指数 p	$M_p=2^p-1$	发现年代	发现者
11	$23\cdot89C$	1536	热格斯
23	$47\cdot178481C$	1640	费尔马
29	$233\ \ 1103\cdot2089C$	1732	欧 拉
37	$223\cdot616318177C$	1640	费尔马
41	$13367\cdot164511353C$	1859	蒲拉那
43	$431\cdot9719\cdot2099863C$	1869	兰 德
47	$2351\cdot4513\cdot13264529C$	1869	兰 德
53	$6361\cdot69431\cdot2094401C$	1869	兰 德
59	$179951\cdot3203431780337C$	1869	兰 德
67	$193707721\cdot761838257287C$	1903	科 尔
71	$228479\cdot48544121\cdot212885$ $833C$	1912	热莫山姆
73	$439\cdot2298041\cdot$ $9361973132609C$	1738	欧 拉
79	$2687\cdot202029703\cdot$ $1113491139767C$	1856	热斯切尔
83	167·5791[illegible]614113275649087721C	1738	欧 拉
97	$11447\cdot$ $13842607235828485645766393C$	1878 1916	勒拉舍
101	素数·素数C		房克姆勃格
103	?	1913	鲍 尔
109	745988807·?	1916	鲍 尔
113	$3391\cdot23279\cdot65993\cdot1868569\cdot$ $1066818132868207C$	1856	热斯切尔
131	263·?	1738	欧 拉
137	?	不详	
139	?	不详	
149	?	不详	
151	$18121\cdot55871\cdot165799\cdot2332951\cdot$ $7289088383388253664437433C$	1912	库尼佛姆

续

指数P	$M_P=2^P-1$	发现年代	发现者
157	852133201 · ?	本世纪初	尤　勒
163	150287 · 704161 · 110211473 · ?	1908	库尼佛姆
167	2349023 · ?	本世纪初	尤　勒
173	730753 · 1505447 · ?	1912	库尼佛姆
179	359 · 1433 · ?	1738	欧　拉
181	43441 · 1164193 · 7648337?	1910	伍德奥尔
191	383 · ?	1738	欧　拉
193	13821503 · ?	本世纪初	尤　勒
197	7487 · ?	1894	库尼佛姆
199	?	本世纪初	尤　勒
211	15193 · ?	1878	勒拉舍
223	18287 · 196687 · 1466449 2916841 · ?	1978	勒拉舍
227	?	本世纪初	尤　勒
229	1504073 · 20492753 · ?	本世纪末	尤　勒
233	1399 · 135607 · 622577 · ?	1856	热斯切尔
239	479 · 1913 · 5737 · 176383 · 134000609 · ?	1738	欧　拉
241	22000409 · ?	1895	毕克默
251	503 · 54217?	1876	鲁卡斯

注　（1）此表中的数据大多是在电子计算机产生之前得到的，近几年的结果没有列入。

（2）末尾有"c"的数字表示已得到完整的因数分解式。

（3）表中发现年代不详的数字，一般是在电子计算机寻找梅森素数时被筛出的合数。

（4）一些数字的因式分解是几位数学家陆续完成的，这里仅给出第一位发现者。

（5）对于$2^{101}-1$，是一个非常有趣的结果，人们仅证明了它必是两个素数之积，并且其中较小的一个至少有11位。但是，大概至今也没有找到这两个素数。

M_{8191}是一个合数，从而否定了“卡特兰猜想”。1957年，又有人证明M_{M17}和M_{M19}分别可被1768（$2^{17}-1$）+1和120（$2^{19}-1$）+1整除。

3.2 $2^{257}-1$与非构造性证明

在梅森数中，最受人关注的数字莫过于$2^{257}-1$。它具有78位数字，是“梅森猜测”中最大的一个数。17世纪梅森曾认为它是素数，但直至本世纪初，数学家们仍然难以证实这一点，早年，也曾引用美联社和纽约时报失实的报道(如 §1.1中美联社的电文，就是谎称克依格博士证明了$2^{257}-1$是素数，云云)，因此就更有“名气”了。当代数学家贝尔曾评论说：一些人对于$2^{257}-1$的喜爱，正如探险者喜爱北极或登山者喜爱珠穆朗玛峰一样。

1922年科瑞特切克曾证明M_{257}是一个合数。但是，大概人们不愿意打破尊崇前人的迷梦，或者对科瑞特切克的证明不理解（他没有给出M_{257}的任何因数），所以这一证明并未得到足够的重视，此后的许多数学书中仍认为M_{257}是素数或作为“猜测”处理。

本世纪初美国出现两位出色的数论大师：D·N·莱赫默和D·H·莱赫默。父子两人曾为数论研究作出许多贡献。例如，他们曾建立一个高达100,000,000的所有数的因数表，还制造了一台因数分解机，证明出许多大数的性质。他们的著作《在数论中捕获“大猎物”》很有影响。尤其是对梅森数，由于D·H·莱赫默改进了鲁卡斯的算法，才使这一法则在确定梅森数中直至今日仍发挥巨大的效应，（详见§3.2）。当然，与世人一样，D·H·莱赫默也十分关注M_{257}的研究，并为此倾注了大量精力。在1931年间，他使用一架台式计算

机花费了700多个小时，最终证明了M_{257}是一个合数。但是，莱赫默也没能找到它的因数。1952年，SWAC计算机也证明了M_{257}是一个合数。它仅用了48秒！但也没有给出因数。

类似于莱赫默等人的证明方法，在数学上一般称为“非构造性证明”。这种方法在数学界是有争议的。它的大意是：对于某事物，即使无法直接找到它，只要利用间接推理确定它的存在，就是有效的证明。我们知道，人类在认识事物的过程中，一般可采取两种认识手段，一是验证，这对于小数量的认识对象是十分有效的。但是，当认识对象的数量非常庞大，甚至无限多时（这在数学中是屡见不鲜的），就需要借助间接的逻辑推理。例如，一个球场有10万个观众座位，并且恰好已坐满而又无站立者。有人问：其中是否有无票者？回答此问题有两种方法，一是逐一检查（这恐怕在球赛结束之后也查不完）；再就是看售出了多少票，从而推算出是否有无票者混入。这后一种方法就是间接推理。莱赫默等人的工作也是如此，他们虽然找不到$2^{257}-1$的因数，却证明了它们存在，这正是“非构造性证明”。对此，数学家韦尔曾形象地描述道：“这种方法的奥妙在于，它仅对人类宣布有某一个珍宝存在，但没有泄露它在什么地方”。

但是，19世纪以来一些数学家（所谓直观主义者）却怀疑非构造性证明在无限意义上的可靠性，因为许多非构造性证明的结果都是很难或者根本无法彻底验证的。无法验证的结果怎能承认其价值呢？人们对于莱赫默等人证明的冷遇正是这种思想的体现。

当代数学家里查兹针对这种“冷遇”，在1978年出版的《今日数学》一书中风趣地写道：

波兰大数学家斯坦豪斯著的《数学一瞥》一书中，有句挑战性的话：78位的数$2^{251}-1$是合数，可以证明它有因数，但这些因数还不知道。我父亲是位富有实践精神的生物学者，他对斯坦豪斯的话斥为无稽之谈——你还不知道数的因数，何以知其有因数？当时我也莫名其妙，但总觉得它相当妙！……事实上如果所含的数目很大（譬如有78位数字），那个所谓"彻底搜查"就是"愚不可及"的了。数学家的"一览无余"不是"逐一枚举"，而是"巧运新思"。

1984年，有人宣称已经完成了$2^{251}-1$的因数分解。但是，笔者至今还没有见到这个结果。

4．公开密码

一般地说，在数学领域中数论是最远离自然界的一个分支。素数以及合数的研究一直被看作最纯粹的数学，并由此赢得"数学皇后"的美誉。但是，本世纪70年代末，事情发生了惊人的逆转，确定素数与大数分解工作突然异常活跃起来。并且，它再不是数学家的孤芳自赏或智力游戏，反而得到许多国家安全部门的极大关注。这是为什么？

原来在1978年，科学家里维斯特、夏米尔和阿德利曼三人发明了一种密码系统，也称RSA系统（这是三位发明者原名Rivest、Shomir和Adleman的字头）。由于这一系统无法破译，所以在短短的几年间就得到一些国家安全部门的广泛应用。最令人惊异的是这种密码的原理竟建立在数学家的无知之上。

我们知道，用现代计算机进行两个大数相乘是件极容易的事。比如，两个101位的素数相乘，使用计算机只须几秒钟。但是反过来，如果不知道这两个素因数，要想完成这个乘积的因数分解，即使用最快的计算机也要几十万亿年的时间。里维斯特等人正是利用了人们在因数分解方面的困难，发明

了一种公开密码。他们的基本思想是：取两个充分大的素数，求出它们的乘积，如果需要发送秘密文电，只须公开告诉发电人这两个素数的乘积，并说明如何用它进行编码，但不必告诉他这两个素数，则任何一个发电人都可以按照编码进行发送秘密文电了。而收电人只要对这两个素因数严守秘密，他就是唯一能破译这一密电的人。当然，这两个素数需要足够的大，以使数学家们无力分解它们。里维斯特等人建议：应使用80位以上的数字才足以扼制因数分解。

RSA密码系统的出现，迅速引起数学界的骚动。其原因有二：一是"数学皇后"——数论的尊严受到了严重的损伤。数学领域中再也不存在"世外桃源"了，几千年来始终"一尘不染"的素数，如今也屈尊在国家安全部门的名下。二是历来"自命清高"的数学家真有些"无地自容"了。一门素称最严整的学科竟让人钻了这么大的空子，该怎样解释呢？正如佐治亚大学的波梅兰斯教授所说："这种密码系统是由于无知而成功的一项应用。它的产生，使更多的人热衷于研究数论了。可以说，对分解因数束手无策的数学家越多，这种密码就越好"。

密码工作人员的言行极大地刺伤了数学家们的自尊心，他们是不会轻易认输的。数学大师希尔伯特早已向世界宣称："在数学之中没有不可知！"从公开密码产生之日起，人们进行因数分解的位数迅速增大，并由此形成了一个新学科——计算数论。1984年2月13日，美国《时代》周刊以"32小时解开3世纪之久未解决的难题——数学家将69位的数字进行因数分解"为题，介绍了美国科学家西蒙斯、戴维斯和霍尔德里奇等人利用克雷计算机进行因数分解的工作。他们从1982

年开始，结合克雷计算机的特点编写了一种因数分解程序，并用它连续分解了50位，60位，63位和67位的数字。此刻，克雷计算机的能力似乎已达到极限。但是西蒙斯等人又向一个具有69位数字的梅森合数进军。他们在一个月里抓住零星时间总共计算32小时12分钟，最后找到了这个梅森合数的全部三个因数：178230287214063289511，61676882198695257501367和12070396178249893039969681。

令人疑惑的是，文中称这个梅森合数是梅森合数表（即素指数$p<257$）中的最后一个，即$2^{251}-1$。这就错了。因为$2^{251}-1$不是69位，而是76位数字。并且，早在1876年鲁卡斯就已经找到$2^{251}-1$的一个因数503；1911年克尼佛姆又找到第二个因数54217。但是至今还没有找到其它因数。这些显然都与西蒙斯等人的结果不同。原因何在呢？笔者根据梅森合数的历史推断，69位的梅森合数应该是$2^{227}-1$，它是本世纪初尤勒用一架台式计算机确定的合数，但是一直没有找到它的任何因数。

数学家们的因数分解能力确实是在突飞猛进。根据1986年末的消息，一些国家已有可能在一天之内分解一个85位以上的数。因此，现在感到不安的不再是数学家了，而是那些得逞一时的国家谍报部门。按照这样的形势发展可以预测：不久之后，RSA密码系统必将被密码破译人员一一侦破，这大概是嘲弄数学家所得到的“报应”吧！不过，无论如何，RSA的产生总算结束了“数论无用”的历史。

第四章 斐波那契数

对外部世界进行研究的主要目的在于发现上帝赋予它的合理次序与合谐，而这些是上帝用数学语言透露给我们的。

——开卜勒

§4.1 《算盘书》与“生小兔问题”

在数学领域中存在着许许多多的数列，但是最有名的要数斐波那契数列了，即

1，1，2，3，5，8，13，21……

其规律是：从第三项开始，每一项都等于它的前两项之和。这一数列中的数字就叫做斐波那契数。

早在公元13世纪，数学家斐波那契在一道有趣的数学题目中建立了这个数列。其后几百年间，人们陆续发现了它的许多奇异的性质，由此名声大振。19世纪，人们为了纪念斐波那契的数学成就，经鲁卡斯提议，将这一数列命名为斐波那契数列。

1. 斐波那契小传

斐波那契是意大利一位著名的数学家。他于1175年生于

比萨 原名叫莱昂纳多，斐波那契是他的绰号（Fibonacci是filiusBonacci的缩写），意为“波那契之子”。大概是为了与15世纪的另一位名叫莱昂纳多的大艺术家相区别，所以斐波那契又称比萨的莱昂纳多。

斐波那契的父亲是一位商人，曾担任意大利一些大商行的海关管理人员。出于经商或接受教育的需要，斐波那契在很小的时候就跟随父亲到过北非的布伊。后来，又旅行到埃及、西西里、叙利亚、希腊和法国南部。由于父亲职业的影响，斐波那契对算术产生了浓厚的兴趣。通过拜访各处学者，使他有机会了解不同国家在商业上的算术体系。经过对比他认为：在众多的算法中，要数印度的阿拉伯数字1，2，3，…最为先进。1202年在他回到比萨不久，即发表了当时最优秀的数学著作《算盘书》。此书的原名是《Liber Abaci》，其中Liber是书；abcus（复数abaci）直译是算盘，原指古希腊人用作计算或画图的沙盘，不是中国的算盘。当时abacus也可当作算术的代名词，所以《算盘书》不是专讲算盘的书，也可以译作《算术书》。这本书共分为15章，其中第1～7章介绍了记数制和整数分数的各种算法；第8～12章是算术在商业上的应用；第13章是线性和二次方程的试位法和代数程序解法；第14章是开平方、开立方法则；第15章是几何度量和代数问题。

当时斐波那契具有很高的声望，他的才能深受神圣罗马帝国国王弗里德里希二世的赏识。据记载：国王曾邀请斐波那契到宫廷参加数学竞赛，由宫廷学者巴勒莫的约翰提出三个问题。第一题：求一数，它的平方加5或减5后仍然是平方数。第二题：求解三次方程$x^3+2x^2+10x=20$。第三题：

解一个不定方程。斐波那契迅速地解出了这些题，使在场的众多学者大为震惊。斐波那契还发表了《几何实用》（1220年）、《象限仪书》（1225年）、《开花》等数学名著，并由此获得“中世纪最杰出的数学家”称号。但是历史学家们分析，斐波那契的实际水平远远高于这些著作的内容。这是因为当时的欧洲没有人能在学识上与他匹敌，所以无法把书写得太深。

大约在1250年斐波那契离开了人世。此后几百年间，由于连年战乱使他出色的工作没能对欧洲的数学研究产生应有的影响。直到16世纪，人们才开始关注他的成果。但影响最大的不是他对印度的阿拉伯数字的引入，而是《算盘书》中的一个貌似平凡的题目：生小兔问题。斐波那契也由此而流芳千古。

2．有生命的数列

原在1228年，斐波那契曾修订了他1202年的著作《算盘书》（现在人们见到的就是这个修订本）。修订本中增加了一个有趣的问题，即“由一对兔子开始，一年后可以繁殖成多少对兔子呢？”文中写道：

“某人把一对兔子放在某处，四周用墙围了起来，看一年后它们总共会有多少对兔子。假设兔子的生殖力是这样的，每一对兔子每一个月可以生一对兔子，而且兔子在出生两个月以后具有生殖后代的能力。在第一个月里第一对兔子生了一对兔子，因而第一个月兔子的总数是两对；在这两对中，只有一对可以在下月里生一对兔子，所以第二个月里共有3对兔子；其中有两对可以在下月里进行生殖；所以在第三个月里有两对兔子出生，在这个月里兔子数目增加到5对；其中有3对在下个月可以生产后代；所以第四个月里兔子增长为8对……，到第十二个月里，兔子总数为377对。”

这个繁殖过程可以通过图4-1表示出来。按照图示的规律就可以逐步确定每个月的小兔数。

实际上，这是一个理想化的“繁殖问题”，其中假定了“小兔不死”以及每次生产皆“一雌一雄”它最初使人感到

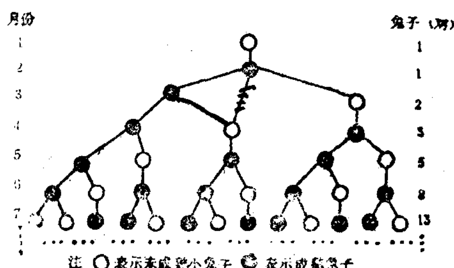


图4-1

惊奇的是兔子的增长速度竟如此迅猛，在短短的12个月里就由一对繁衍成377对！难怪当代科学家在讲述“人口问题”时，仍以斐波那契的“生小兔问题”为例。让人们从中领悟人口激增的“可怕性”。但是，这个故事的重要性并非仅在于此 在斐波那契提出此问题的几百年之后人们在科学研究中惊奇地发现：这种“小兔繁殖”的规律还存在于大量的自然现象之中。

首先是在16世纪，德国科学家开卜勒在研究“叶序”问题时，得到了与斐波那契数列有关的数字。原来植物的叶子在茎上的排列是有一定规则的。若把位于茎周同一母线上的两片叶子叫做一周期的话，那么

$$W=\frac{\text{每个周期叶子绕的圈数}}{\text{每个周期里的全部叶子数}}$$

是一个定数，它仅随植物品种的不同而不同。

例如

榆树的叶序一周期有两片叶子，且一周期叶子仅绕一圈。所以$W_{榆}=\frac{1}{2}$。

山毛榉一周期有三片叶子，所以$W_{山}=\frac{1}{3}$。

樱桃（橡树等）的叶子排列如图4-2，可知

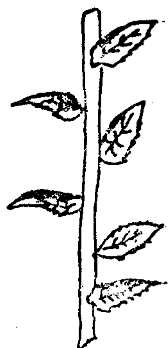


图4-2

$W_{樱}=\frac{2}{5}$。

还有，

$W_{梨}=\frac{3}{8}$，

$W_{柳}=\frac{5}{13}$，等等。

将这些貌似杂乱无章的数字排列起来：

$$\frac{1}{2}, \frac{1}{3}, \frac{2}{5}, \frac{3}{8}, \frac{5}{13}, \cdots\cdots$$

你会发现，这些分数的分子和分母都恰好各自构成一个斐波那契数列。

再如，本世纪初数学家泽林斯基在一次国际数学会议上提出一个"树木生长问题"：如果一棵树在1年以后长出一

条新枝，然后总是休息一年，再在下1年又长出一条新枝，并且每一条树枝都按照这个规律长出新枝（如图4-3）。那么，在第1年只有主干，第2年有2枝，第3年有3枝，第4年有5枝，然后是8枝，13枝，等等。显然，树枝的繁殖方式也是按照斐波那契数增长的，这只是“生小兔问题”的变化而已。

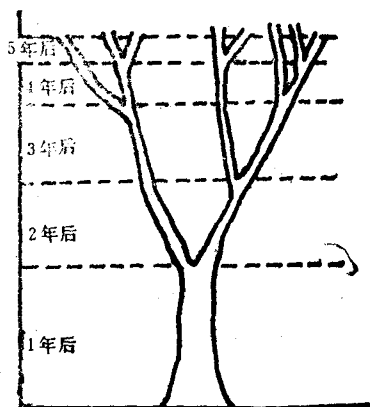
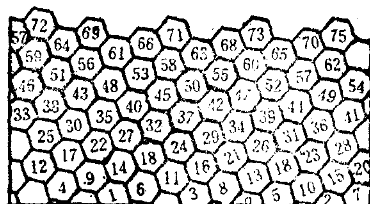
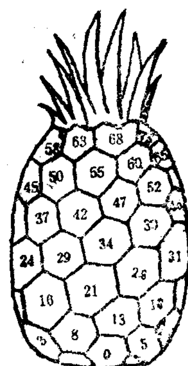


图4-3

还有一些产生斐波那契数列的例子，现略述如下：

（1）菠萝的鳞片：如图4-4（1），将一个菠萝放在一个





（1）　　　　2）

图4-4

平面上，测量它的鳞片（六边形）中心与所在平面的距离（按照某一个比例单位）把它们填在各自的鳞片上。再将菠萝的表皮在平面上展开（如图4-4（2）），就会发现，在三个方向上的数字构成等差数列。即

0，5，10，15，20，……（公差：5）

0，8，16，24，32，……（公差：8）

0，13，26，39，52，……（公差：13）

显然，它们的公差5，8，13恰好是斐波那契数列中的三项。

（2）蜜蜂进房：如图4—5，一只蜜蜂从蜂房A出发，想爬到第1，2，…，n号蜂房，只允许它自左向右走（不许反向倒走），那么它爬到各蜂房的方式（即路线）也构成一个斐波那契数列。

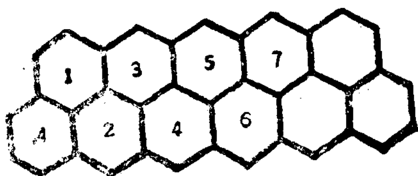


图4-5

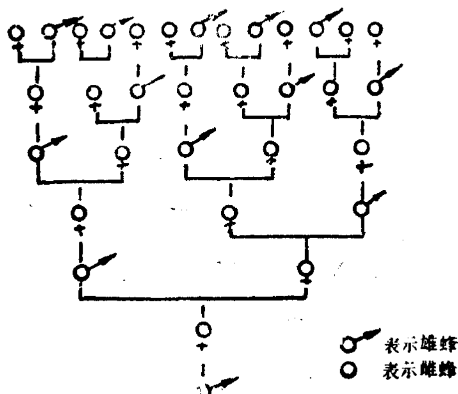


图4-6

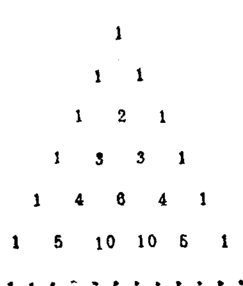
（3）雄蜂家族：一只雄蜂的家族，其每一代祖先的数目也构成一个斐波那契数列。如图4-6，按照蜜蜂的繁殖规律，一只雄蜂仅有一个母亲，没有父亲，所以两代的数目皆为1；而这只雄蜂的母亲（雌蜂）必有一父一母，* 所以第3代的数目是2；而第3代的雄蜂又仅有母亲，雌蜂则有一父一母，所以第4代的数目是3，……它们恰好形成一个斐波那契数列。

以上的例子都是与生物学有关的问题，这种现象在生物学中称为“鲁德维格定律”。其实，斐波那契数列还大量地出现在其它类的问题之中。下面再看几个例子。

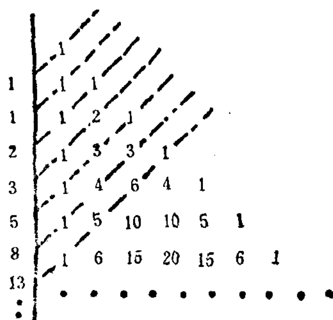
（4）上楼方式问题：上楼梯时，若允许每次跨一阶或两阶，那么，对于楼梯阶数为1，2，3，4，…时，上楼的方式种数恰好构成斐波那契数列：

1，2，3，5，8，……

（5）杨辉三角形：图4-7(1)中由数字组成的三角形叫扬



（1）



（2）

图4-7

---

* 因为雄蜂是由未受精卵孵化而成的，所以只有母亲；而雌蜂是由受精卵孵化的，所以有一父一母。

辉三角形，它最早出现在杨辉所著的《详解九章算术》一书中。在国外也称为帕斯卡三角形。它反映了二项式$(a+b)^n$ $(n=1,2,\cdots)$的展开式系数的规律，在数学中非常著名。如果我们将它改写成图4-7(2)中的形式，就会发现，若将图中虚线（称之为递升对角线）上的数字相加，也会得到斐波那契数列。

此外，在几何学、代数学以及概率论中，也有许多与斐波那契数列有关的例子，对此我们将在下一节中介绍。

一个理想化的"生小兔问题"竟然在众多的自然现象中时时显露出它内在的"数学魅力"，真有些不可思议。细想下去，它会使人在有意与无意之间，恍然步入一个神奇的境界。那里隐含着大自然的内在规律，它们被形形色色的现象所掩盖着，人类的认识还远远没有把握住它们，只是在苦苦的探索中时而发现一些凤毛麟角，而斐波那契数——这似乎有生命的数字，是否就是大自然生命之源的一部密码呢？这个问题目前还回答不了。不过，它确实是太玄妙了！

§4.2 数学性质

从上一节生动的例子中我们已经看到：斐波那契数列的递增速度很快。如果按照图4-1所示的方法，逐步确定第二年、第三年、…的兔子数，显然非常困难。那么，是否有办法找到它的递增规律，从而很快地确定某个月的小兔数目呢？这正是数学家要完成的工作。

1634年，奇拉诗首先留意于"生小兔问题"。他在细心的观察中发现：若将每月出生的小兔对数记为u_n（n代表月

序数），则对于斐波那契数列

$\{u_n\}$：1，1，2，3，5，8，13，…

显然有递推关系

$$u_{n+1}=u_n+u_{n-1},$$

即数列中的每一项数字都等于它的前两项之和。这个式子说明：第$n+1$个月的兔子可分为两类，一类是第n个月时的兔子；另一类是当月新生的兔子，这些恰好等于第$n-1$个月时的兔子数，因为第$n-1$个月的兔子到第$n+1$个月时均可生殖了。

奇拉特的工作使“生小兔问题”上升为形式化的数学问题，从而拉开了斐波那契数列研究的序幕。于是，数学家们从这里开始起步了。

1．通项公式

我们知道，如果一个数列$\{a_n\}$的第n项a_n与n之间的关系可用一个公式来表示，这个公式就叫做这个数列的通项公式。

那么，斐波那契数列的通项公式是什么呢？这个问题早在18世纪就提出来了，并已经得到解决。它的结果不止一个，而且形式都非常有趣。请看如下几例：

（1）**比内公式**：设u_n是斐波那契数列的第n项，则

$$u_n=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right]。$$

注　这个公式最早载于18世纪棣美佛的《分析集锦》一书中，它的最初证明是由数学家比内完成的，所以又称比内公式。值得指出的是，这个公式的左端为正整数，右端却由无理数表出，多么完美的结合！

证明　用数学归纳法。

当$n=1$时，直接验算可证等式成立。

设$n\leqslant k$时，结论成立。现在推证$n=k+1$时，结论成立。

$$u_{k+1}=u_k+u_{k-1}$$

$$=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k-\left(\frac{1-\sqrt{5}}{2}\right)^k\right]$$

$$+\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}-\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right]$$

$$=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left(\frac{1+\sqrt{5}}{2}+1\right)\right.$$

$$\left.-\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\left(\frac{1-\sqrt{5}}{2}+1\right)\right]$$

$$=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left(\frac{1-\sqrt{5}}{2}\right)^2\right.$$

$$\left.-\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(\frac{1-\sqrt{5}}{2}\right)^2\right]$$

$$=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+1}-\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right].$$

所以，对于$n=k+1$时，结论成立。从而公式得证。

(2) 矩阵表示法：设

$$A=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$$

则
$$A^n=\begin{pmatrix}u_{n-1} & u_n\\ u_n & u_{n+1}\end{pmatrix},$$

其中的u_n就是斐波那契数列的第n项。

(3) 行列式表示法：

$$u_{n+1}=\begin{vmatrix} 1 & -1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & -1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \end{vmatrix}$$

等式的右端是一个n阶行列式。

(4) 组合数表示法：

$$u_{n+1}=C_n^0+C_{n-1}^1+C_{n-2}^2+\cdots+C_{n-k}^k{}^*$$

其中$k=\left[\frac{n}{2}\right]^{**}$ $(n=1, 2, \cdots,)$。

注 对于通项公式(2)~(4)，已涉及到高等数学知识，所以本书略去它们的证明，仅列出结果，用以说明斐波那契数列的奇趣。详见《斐波那契数列》(吴振奎著，辽宁教育出版社，1987)。

应当指出，虽然找到了斐波那契数列的通项公式(并且种类繁多)，但是要想确定一个较大的斐波那契数(即某一年的小兔数目)，仍然不是一件轻松的事。你只要一动手就会知道，每一个通项公式的运算都相当繁杂，难尽人意。1962年10月，美国《数学趣味杂志》宣布：有人利用IBM7090

---

* C_n^m是组合符号，即$C_n^m=\frac{n(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdot 3\cdots\cdots m}$.

这里约定，$C_n^0=1$；当$n<m$时，$C_n^m=0$。

** $[x]$表示不超过x的最大整数。例如，

$\left[\frac{1}{2}\right]=0$，$[2]=2$，$\left[1\frac{1}{3}\right]=1$，等等。

计算机试求了u_{571}的值，它大约是47年后的小兔对数，得到结果

$$u_{571}=9604120061892255382394288333092486502610 4917411877067816822264789029014378330847336419258908 4185254331637646183008074629。$$

不久，该杂志又宣称找到了新的斐波那契数u_{1000}，这是一个209位数字的巨数！由此可见，这项工作绝不是手算所能及的事。

2．数字关系

总体来说，斐波那契数列最诱人的性质还是它们数字间的奇妙关系。不知为什么，一个孤独的自然数一旦是斐波那契数列中的一员，就与其它数字神奇般地结合了起来。下面我们逐一介绍斐波那契数列的数字关系，并且给出部分等式的证明。

（1）1680年，卡西尼利用奇拉特公式证明：

$$u_{n+1}u_{n-1}-u_n^2=(-1)^n\ (n\geqslant 2)。$$

证明　用数学归纳法。

当$n=2$时，$u_{n-1}=u_n=1$，$u_{n+1}=2$，所以$2\times 1-1=1$，等式成立。

设$n=k$时等式成立．再证$n=k+1$时，等式成立．

$$\begin{aligned}u_{n+1}u_{n-1}-u_n^2&=u_{k+2}u_k-v_{k+1}^2\\&=(u_{k+1}+u_k)u_k-(u_k+u_{k-1})^2\\&=u_{k+1}u_k+u_k^2-u_k^2-2u_ku_{k-1}-u_{k-1}^2\\&=u_k^2+u_{k-1}u_k-2u_ku_{k-1}-u_{k-1}^2\\&=u_k^2-u_{k-1}^2-u_ku_{k-1}\\&=u_k^2-u_{k-1}(u_{k-1}+u_k)\end{aligned}$$

$$
\begin{aligned}
&=u_k^2-u_{k-1}u_{k+1}\\
&=-\left(u_{k-1}u_{k+1}-u_k^2\right)\\
&=-(-1)^k=(-1)^{k+1}.
\end{aligned}
$$

所以公式成立。

注 这个公式的推广形式是

$$u_{n-k}u_{m+k}-u_nu_m=(-1)^nu_{m-n-k}u_k$$

(2) 除奇拉特给出的公式之外，人们还发现了斐波那契数列项数间更一般的关系：

$$u_{m+n}=u_{n-1}u_n+u_nu_{m+1}.$$

例如，$m=1$时，有$u_{n+1}=u_{n-1}u_n+u_nu_2=u_{n-1}+u_n$，这显然就是奇拉特公式。

(3) 第奇数（$2n+1$）个斐波那契数满足等式：

$$u_n^2+u_{n+1}^2=u_{2n+1}.$$

(4) 第偶数（$2n$）个斐波那契数满足等式：

$$u_{n+1}^2-u_{n-1}^2=u_{2n}.$$

(5) 当斐波那契数的序数是3的倍数时，这一项满足等式：

$$u_{n+1}^3+u_n^3-u_{n-1}^3=u_{3n}.$$

性质(2)～(5)的证明都比较容易，现仅给出(4)的证明。

证明 (4) 根据性质(2)，设$m=n$，则有

$$
\begin{aligned}
u_{2n}&=u_{n-1}u_n+u_nu_{n+1}=u_n\left(u_{n-1}+u_{n+1}\right)\\
&=\left(u_{n+1}-u_{n-1}\right)\left(u_{n+1}+u_{n-1}\right)\\
&=u_{n+1}^2-u_{n-1}^2.
\end{aligned}
$$

(6) 如果n是偶数，则

$$\frac{1}{u_n}=\frac{1}{u_{n+1}}+\frac{1}{u_{n+2}}+\frac{1}{u_n u_{n+1} u_{n+2}}.$$

例如，当$n=4$时，

$$左端=\frac{1}{3};$$

$$右端=\frac{1}{5}+\frac{1}{8}+\frac{1}{120}$$

$$=\frac{40}{120}=\frac{1}{3}=左端。$$

(7) 本世纪60年代初，美国《数学月刊》登载了罗莱特提出的一道征答题：斐波那契数列中有几个完全平方数？是有限个还是无穷多个？

所谓完全平方数是指可以表示成一个正整数的平方的数。例如，$1=1^2$，$4=2^2$，所以1和4都是完全平方数。在斐波那契数列

1，1，2，3，5，8，13，21，34，55，89，144，…

中，经验证可知$u_1=u_2=1$与$u_{12}=144=12^2$是完全平方数。是否还有其它的完全平方数呢？1963年，韦德林曾用计算机检验了直到$n<10^6$的斐波那契数u_n，仍然没有找到新的完全平方数。最后，美国数学家威勒与我国数学家柯召、孙琦分别在1964年和1965年各自独立地证明：斐波那契数列中的完全平方数只有u_1、u_2和u_{12}。

(8) 对于任意正整数m，在前m^2个斐波那契数列中，必有一个斐波那契数可被m整除。

例如，取$m=2$，则$m^2=4$，斐波那契数列的前四项数字是1，1，2，3，显然$m|u_3$。

(9) p是素数且$p\neq5$，则u_{p-1}和u_{p+1}中必有一个是p的倍数。

例如，$p=7$是素数，$u_6=8$，$u_8=21$，显然$u_8=3.7$是p的倍数。

(10) 在斐波那契数列中，$u_m|u_n$的充要条件是mn。

(11) 一个斐波那契数除以另一个斐波那契数的余数，其绝对值仍是一个斐波那契数。

例如，$u_5=5$，$u_7=13$，13除以5余2，显然是数列中的第三项u_3。

(13) 由斐波那契数的尾数组成的数列是循环的，它的循环周期$T=60$，即每经过60个斐波那契数之后，它们的尾数就开始重复一个新的循环。这60个数的尾数是：

1，1，2，3，5，8，3，1，4，5，9，4，3，7，0，7，7，4，1，5，6，1，7，8，5，3，8，1，9，0，9，9，8，7，5，2，7，9，6，5，1，6，7，3，0，3，3，6，9，5，4，9，3，2，5，7，2，9，1，0，…

再往下(从第61个数开始)的尾数又重复出现1，1，2，……，即进入第二循环。

以上我们简要地列举了斐波那契数的一些性质，限于篇幅和知识范围，没能逐一给出它们的证明。虽然人们在斐波那契数的研究上花费了很大精力，但是仍然存在着一些无法解决的问题。例如，

(1) 斐波那契数列中的素数是有限个还是无穷多个？

到目前为止，人们仅发现$n=3$，4，5，7，11，13，17，

23，29，43和47时，u_n是素数，其中$u_{47}=2971215073$。但无力确定是否还有其它素数。从已知的结果中可知：当n是大于4的素数时，u_n不一定是素数。比如$n=19$是素数，而$u_{19}=4181$却是合数。但是反过来，当u_n是素数时，除$n=4$之外，其它的n值一定是素数吗？

（2）斐波那契数列中的三角数是有限个还是无穷多个？

所谓三角形数的数列是

1，3，6，10，15，21，28，36，45，55，…

它的通项公式为$n(n+1)/2$（详见本书第八章 形 数）。显然，三角形数1，3，21，55都是斐波那契数。是否还有其它的三角形数是斐波那契数？这个问题至今还没有解决。但是人们却证明了一个有趣的结果，即：对于斐波那契数列中的三角形数，它的所在项数恰好等于其在三角形数数列中所在项数的只有1和55。例如，55在斐波那契数列中处于第10位，而它在三角形数的数列中所处的位置也是第10位。

§4.3 数 学 地 位

斐波那契数列在数学中占有重要地位，它的影响远远超出了数论的范筹，在许多科学领域中发挥着奇妙的作用。本节将概括地介绍一下斐波那契数列与一些数学分支的联系以及它的一些应用。

1．与其它数学知识的联系

（1）1753年希姆松发现斐波那契数列的前后两项之比u_{n+1}/u_n恰好是连分数

$$1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ddots}}}$$

的第n个渐近分数*．（进一步可以证明，u_{n+1}/u_n的极限就等于这个连分数．）

这一性质可由奇拉特公式和辗转除法推出，即

$$\frac{u_{n+1}}{u_n}=\frac{u_n+u_{n-1}}{u_n}=1+\frac{u_{n-1}}{u_n}$$

$$=1+\cfrac{1}{\cfrac{u_n}{u_{n-1}}}=1+\cfrac{1}{1+\cfrac{u_{n-2}}{u_{n-1}}}$$

$$=1+\cfrac{1}{1+\cfrac{1}{\cfrac{u_{n-1}}{u_{n-2}}}}=\cdots$$

$$=1+\cfrac{1}{1+\cfrac{1}{1+\ddots\cfrac{}{1+\cfrac{1}{1}}}}$$

---

* 对于连分数$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots}}$，它的第一、第二、…个渐近分数分别是$a_0$，$a_0+\frac{1}{a_1}$，等等。

（2）黄金分割：如图4-8，若P点将线段AB分为大小不同的两段，且小段与大段之比恰好等于大段与全长之比，即



图4-8

$$PB : AP = AP : AB,$$

则称P点分线段AB成中外比.这是一种奇妙的比例，它在绘画艺术和建筑上都有着非凡的作用。所以中世纪意大利艺术家达·芬奇称之为黄金分割。

如果设$AB=1$，且$AP=x$，则可以求得

$$x=\frac{\sqrt{5}-1}{2}=0.618\cdots,$$

这个数叫做黄金数。有趣的是斐波那契数列的前后两项之比的极限

$$\lim_{n\to\infty}\frac{u_n}{u_{n+1}}$$

恰好等于黄金数。这一结论可从下面的比值（u_n/u_{n+1}，$n=1, 2, 3, \cdots$）中看到：

$$\frac{1}{1}=1.0000 \qquad \frac{1}{2}=0.5000$$

$$\frac{2}{3}=0.6667 \qquad \frac{3}{5}=0.6000$$

$$\frac{5}{8}=0.6250 \qquad \frac{8}{13}=0.6154$$

$$\frac{13}{21}=0.6190 \qquad \frac{21}{34}=0.6176$$

$$\frac{34}{55}=0.6182 \qquad \frac{55}{89}=0.6180$$

$$\frac{89}{144}=0.6181 \qquad \frac{144}{233}=0.6180$$

等等，这个比值最终逼近于黄金数0.618…。

注 这一性质的严格证法较多，也可利用斐波那契数列与连分数的关系证明。大体方法是：设

$$x=1+\cfrac{1}{1+\cfrac{1}{1+\ddots}},$$

则$x-1=\dfrac{1}{1+(x-1)}$，即$x^2-x-1=0$。解得$x=\dfrac{1}{2}(1\pm\sqrt{5})$（负值舍去）。根据上述性质(1)可证$\lim\limits_{n\to\infty} u_n/u_{n+1}=x$，所以

$$\lim_{n\to\infty}\frac{u_{n+1}}{u_n}=\frac{1}{x}=\frac{\sqrt{5}-1}{2}=0.618\cdots.$$

(3) 三角形的边长：是否存在以互异的斐波那契数为边长的三角形？

这是不可能的。根据斐波那契数的数间关系：

$$u_1=u_2=1,\ u_{n+1}=u_n+u_{n-1}\ (n\geqslant 2).$$

现取数列中的任意三项$u_l<u_m<u_n$，可以证明$u_n\geqslant u_l+u_m$，这与"三角形的任一边小于其它两边之和"的定理相矛盾 所以它们不能构成一个三角形。

注 还可以证明：顶点坐标分别是

$$(u_n,\ u_{n+1},\ u_{n+2}) \quad (u_{n+3},\ u_{n+4},\ u_{n+5})$$

$$(u_{n+6},\ u_{n+7},\ u_{n+8}) \quad (u_{n+9},\ u_{n+10},\ u_{n+11})$$

的四面体体积为零。

(4) 概率："连续抛一枚硬币，直到连续出两次正面为止"的事件发生在第n次抛掷所有可能的方式数为u_{n-1}。

如果用H表示硬币的正面，用T表示硬币的背面，请看下表：

n	可能的方式	不同方式的种数
2	HH	1
3	THH	1
4	HTHH TTHH	2
5	THTHH HTTHH TTTHH	3
6	HTHTHH TTHTHH THTTHH HTTTHH TTTTHH	5
…	…………	…

显然$n=2$，3，4，…时，所有可能的方式数恰为斐波那契数1，1，2，3，5，…。

2．应用种种

斐波那契数列的最早应用出现在1884年，当时法国的拉姆利用它证明了一个定理："应用辗转相除法（欧几里得除法）的步数（即辗转相除的次数）不大于较小数的位数的5倍。"此后，人们开始留心斐波那契数列的作用，得到许多有趣的结果。

(1) 正方形铺满平面问题：取边长分别为1，2，3，…的正方形，问用它们是否能铺满整个平面？

这个问题至今尚未解决。但是人们借用斐波那契数列证明了：用边长为1，2，3，…的正方形，至少可以铺满整个平面的四分之三。它的基本方法如图4-9，用斐波那契数列1，2，3，5，…为边长的正方形可以铺满坐标平面的第四象限；

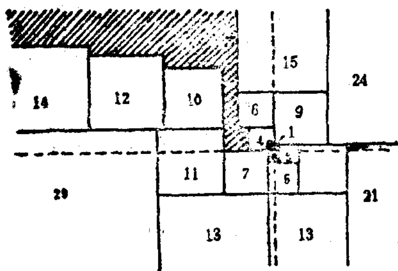
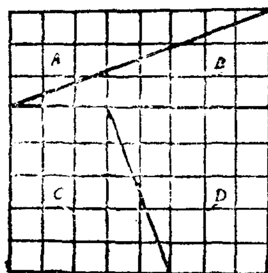


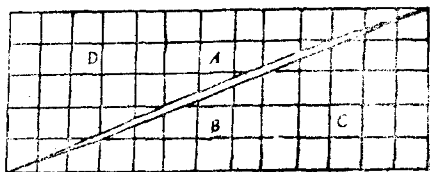
图4-9

用推广的斐波那契数列(4)，(6)，9，15，24，…为边长的正方形可以铺满坐标平面的第一象限：用推广的斐波那契数列7，11，18，29，…为边长的正方形可以铺满坐标平面的第三象限；还有没在上述数列中出现的数字4，6，10，12，14，…等为边长的正方形放在第二象限。由图4-9可见，用以1，2，3，…为边长的正方形至少可以铺满平面的四分之三。

(2) 拼图游戏：把一个边长为8的正方形按照图4-10(1)的方式剪裁，然后拼成图4-10(2)的矩形，结果一个面积为



(1)



(2)

图4-10

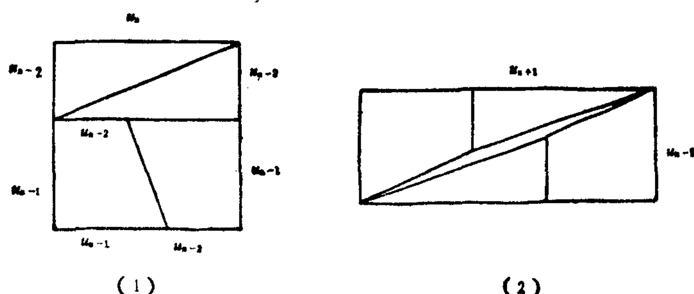
$8^2=64$的正方形，竟拼成了一个面积为$13\times5=65$的长方形（多出了一个单位）！原因何在呢？仔细观察就会发现：图4-10(2)的长方形是有缝的。

原来正方形和矩形的边长8，5，13恰好是斐波那契数列中的三项，由公式

$$u_n^2-u_{n-1}u_{n+1}=(-1)^{n+1} \qquad (*)$$

可知，上述的拼剪相当于$n=6$时，$u_6=8$，$u_5=5$，$u_7=13$。u_n^2是正方形面积，$u_{n-1}u_{n+1}$是长方形的面积、它们之间恰好相差一个单位数（有时也会少一个单位）。

使用公式(*)还可以得到这类拼图游戏的一般方法：任取三个斐波那契数u_{n-1}，u_n，u_{n+1}，将以u_n为边长的正方形按



(1)　　(2)

图4-11

照图4-11(1)中的方式剪开，可以拼成一个边长分别是u_{n-1}、u_{n+1}的长方形（如图4-11(2)）。则当n是偶数时，长方形比原正方形多一个单位；当n是奇数时，长方形比原正方形少一个单位。例如，取13为边长做正方形，把它剪成边长为8和21的长方形，又会出现与图4-10类似的结果。但这次是少了一个单位（即接缝处有重叠）。

（3）象棋马步跳法：一般的人都知道，在象棋中马走“日”字。其原因是按照这种步法，马能遍及整个棋盘上的任何一点。这一问题已经得到严格的数学证明。但是，有一个广义的马步遍及问题，即考虑一个每步横跳m格、纵跳n格的马，它能否跳遍棋盘上的所有点？这种马称为广义（m,n）马。显然，走“日”的马是（1，2）马。

1981年，我国学者胡久稔给出两个有趣的结果：如
12，

①对于（$n,n+1$）马，
P可用$2n+1$步达到。

②若相邻两个斐波那契数u_{n-1}、u_n一奇一偶，则（u_{n-1},u_n）马可用u_{n+1}步从O跳到P点。

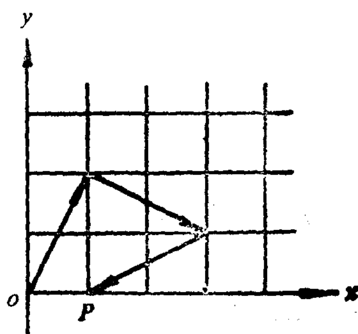


图4-12

对于性质②，我们举例说明一下：如图4-13，一个（2，3）马要从O点跳到P点，它的步法是：$O\to L\to M\to N\to Q\to P$，恰好是5步，与性质②所述相符，实际上，这个（2，3）马跳的是“用”字，它是朝鲜象棋中马的跳法。

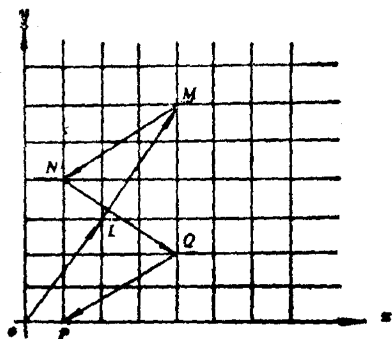


图4-13

（4）斐波那契数列的推广及应用：斐波那契数列的推广

工作是在1876年由鲁卡斯首创的。当时，鲁卡斯为了研究梅森数的性质，给出了第二类斐波那契数列：

1，3，4，7，11，18，…

它的数间关系是：

$$v_1=1,\ v_2=3,\ v_{n+1}=v_{n-1}+v_n\ (n\geqslant 2)。$$

通项公式是：

$$v_n=\left(\frac{1+\sqrt{5}}{2}\right)^n+\left(\frac{1-\sqrt{5}}{2}\right)^n。$$

并且，这类数列与斐波那契数列存在关系：

$$v_n=\frac{u_{2n}}{u_n}。$$

鲁卡斯利用第二类斐波那契数列（亦称鲁卡斯数列）给出了一系列重要定理，在梅森数乃至当代计算机确定素数的研究中发挥了巨大的作用（详见本书第三章梅森数）。

以上我们介绍了斐波那契数列的各种联系和应用，但这仍然仅是一小部分。遍览广阔的数学领域，在几何学、代数学、集合论、数值积分、计算机科学等许多学科中，都会找到斐波那契数列的“足迹”。尤其是本世纪50年代，由于“优选法”的产生，斐波那契数列以它奇妙的递推关系在众多的算法中独树一帜，世称斐波那契（数列）算法。于是围绕斐波那契数列的研究更加活跃起来。60年代，国外甚至出现了专门性杂志《斐波那契季刊》。

从“生小兔问题”出发，我们的思路已经走得很远很远，但又似乎搞得“很乱很乱”。在无垠的大自然中，斐波那契数列

1, 1, 2, 3, 5, 8, 13, 21, 34, …

宛如一条神奇的游龙若即若离，似有似无。时而在冥冥中跃然纸上，时而在沉静里渺然无迹。凡是了解它的人无不慨叹：知其然，不知其所以然！是啊，这貌似平凡的数列竟有如此大的影响和蕴力，这始终还是一个未知数！不过总有一天，人类思维升华，会使人们再居高临下，俯瞰那五彩缤纷的世界，认识自然界的各种规律性。如果你再留心于"斐波那契（数列）现象"，定会看到一个"游龙戏水"的奇观。

第五章　费尔马数

虽然（上帝）不允许我们看透自然界本质的奥秘，从而认识现象的真实原因。但是，却可能发生这样的情况：一定的虚构假设足以解释许多现象。

——欧　拉

§5.1　从寻找素数谈起

费尔马数是指形如$2^{2^n}+1$的数字，其中n取正整数，通常记为F_n。由于它的产生和发展新奇而又出人意料，所以在数论中非常著名，我们知道，许多数论问题都是围绕着素数被提出来的。费尔马数也不例外，它是人们寻找"素数公式"的产物。

1．素数是无限多的

所谓"素数公式"是数学家们一个由来已久的愿望，即找出一个关于n的函数，当n取从0至无限大的整数时，给出所有的素数。这个问题的先声是"确定素数的个数"问题，人们发现自然数中存在着许许多多的素数，但是究竟有多少个素数？它们是有限的还是无限多的？这是一个非常古

老的问题。通常筛选人们发现：

在1～1000之间有168个素数，

在1000～2000之间有138个素数，

在2000～3000之间有127个素数，

在3000～4000之间有120个素数，

在4000～5000之间有119个素数，

等等。这一结果说明：素数的分布是不规则的，并且越往上越稀少。不过早在古希腊时期，欧几里得在《几何原本》第九篇命题20中已经指出：素数的个数比任何指定的数目都要多。换言之，即“素数的个数是无限多的”。文中欧几里得给出了一个非常优美的证明，现略述如下：

证明 用反证法。假如素数是有限多的，现设全部素数为

$$p_1, \ p_2\cdots, \ p_k.$$

令$q=p_1p_2\cdots p_k-1$，则如果q是素数，由于q必大于每一个p_i（$i=1, 2, \cdots, k$），所以q将是一个异于p_i的素数，与题设矛盾。

如果q是合数，则它必有素因数。往证：任何一个p_i（$i=1, 2, \cdots, k$）都不能整除q。如若不然，设$p_i \mid q$，虽然又有$p_i \mid p_1p_2\cdots p_k$（因为$p_i$是其中之一），从而有$p_i \mid (p_1p_2\cdots p_k-q)$。根据所设可得$p_i \mid 1$，而$p_i$是素数，矛盾。故任何一个$pi$均除不尽$q$，这说明$q$有不同于$p_1, p_2, \cdots, p_k$的素因数，与$p_i$（$i=1, 2, \cdots, k$）是全部素数的题设矛盾。所以原命题成立。

注 这个定理不但自身在数论中非常重要，而且还是“非构造性证明”（见 §3.3）的一个最早的例证。因为在无限的自然数中，谁能真正地数一数素数有多少个？欧几里得却利用严格的逻辑方法巧妙

地证明了这一点，这大概就是数学家的“超人之处”吧！

欧几里得证明引发了人们寻求素数规律的热望。既然素数是无限多的，那么能否找到一个不遗漏且唯一地给出素数的公式呢？这是一个十分诱人的问题。假如找到了这样的公式，那时再寻找某一个素数或构造长长的素数表就会方便多了。人们将摆脱盲目的试除之苦，为确定某数是素数还是合数，只须把它代入公式就会一目了然。怀着这样的愿望，数学家们从欧几里得时代起就开始了寻找。在漫长的岁月里，许多奇妙的“素数公式”纷纷出现，其结果使人扑朔迷离。这些形形色色的“素数公式”丰富了数学宝库（对于这些有趣的工作及结局，我们将在本节末介绍）。而费尔马数公式正是这众多的结果之一

2．费尔马的故事

费尔马是一位非常著名的数学家，他于1601年8月20日出生在法国南部的土鲁斯附近的波蒙。他的正式职业是律师，后任法官和土鲁斯议会议员。研究数学问题只是他的业余爱好。但是在广阔的数学领域中到处耸立着费尔马的丰碑，他几乎是一位数学全才．也称“业余数学家之王”和“数论之父”。然而，大概出于“业余”的缘故，费尔马从不发表数学论著，只将自已的心得记在所读书籍的空白“天地”处，或通过信件转告好友。并且他的大部分结果言简意赅，只给出略证或根本未证。“费尔马数公式”正是在这样的背景下产生的。

原来数论中有这样一个定理：如果2^m+1是素数，则必有$m=2^n$。

证明　如果m有一个奇数真因数q，则$m=qr$，且

$$2^m+1=2^{qr}+1=(2^r)^q+1$$
$$=(2^r+1)(2^{r(q-1)}-\cdots-2^r+1)。$$

因为$1<2^r+1<2^m+1$，所以2^m+1有真因数2^r+1，即不是素数，矛盾。所以m不能有奇数真因数，仅有$m=2^n$。

但是反过来说，形如$2^{2^n}+1$的数是否一定是素数呢？1640年费尔马在致福兰尼克尔的一封信中说，可以验证当$n=0, 1, 2, 3, 4$时，$2^{2^n}+1$分别等于3,5,17,257和65537，它们都是素数。由此推测：形如$2^{2^n}+1$的数都是素数。当时费尔马无力给出证明，1654年他还曾请帕斯卡证明这一点，也未能成功。1659年，费尔马又信告卡克威说他用一种"最速下降法"证明了这个结果，不过没有人见到他的证明。由于费尔马崇高的数学声望和这类数字验证的艰距性，在很长一段时间里没有人怀疑这一猜想的正确性，并且把它命名为费尔马数，记为：

$$F_n=2^{2^n}+1。$$

注 后人分析，根据费尔马的数学洞察力，他是不会仅由头几个素数值就贸然断定F_n都是素数的。他可能是受到费尔马小定理的逆定理的困惑。这个逆定理是：如果$p \mid 2^p-2$，则p是素数。可以证明任何F_n都可整除$2^{F_n}-2$，所以费尔马坚定了F_n是素数的决心。但实际上这个逆定理是不成立的（当时费尔马等人不知道），它会产生伪素数！这方面的内容详见本书第六章伪素数。

3. 欧拉的工作

一百年后，瑞士科学家欧拉的诞生使问题发生了急剧的逆转。费尔马与欧拉之间存在着一种奇妙的关系，他们在学术上的吻合就象上帝的有意安排一样。前面提到，费尔马的

一生中从未发表过数学著作，并且他给出的绝大部分定理都没有证明。在他逝世后的近百年中也很少有人能解决它们。但是当欧拉出现之后，一切问题都冰释了，他几乎独占地解决了费尔马留下的全部问题（尤其是数论问题），为完善费尔马的数学思想作出了非凡的贡献，赢得了许多荣誉。所以有人把欧拉喻为费尔马“跨时代的知音”。对于费尔马数问题，欧拉也作了深入的研究，但这一次他没能为费尔马赢得荣誉，却发现了重大的错误。

据1729年哥德巴赫介绍，欧拉很早就注意到费尔马数问题，他曾给出相关的两个性质：

（1）任何费尔马数F_n都没有小于100的因数。

（2）任意两个费尔马数都没有公因数。

证明 仅给出（2）的证明。这实际上就是求证：当$k>0$时，$(F_n, F_{n+k})=1$。

设正整数$m \mid F_n$且$m \mid F_{n+k}$，令$a=2^{2^n}$。则利用首项为-1，公比为$-a$的等比数列的求和公式得

$$\frac{F_{n+k}-2}{F_n}=\frac{2^{2^{n+k}}-1}{2^{2^n}+1}=\frac{a^{2^k}-1}{a+1}$$

$$=a^{2^k-1}-a^{2^k-2}+\cdots+a-1,$$

所以$F_n \mid (F_{n+k}-2)$。由于$m \mid F_n$，因此$m \mid (F_{n+k}-2)$。再由$m \mid F_{n+k}$可得$m \mid 2$。但是费尔马数都是奇数，所以必有$m=1$。于是证明了$(F_n, F_{n+k})=1$。即在数列

$$F_0, F_1, F_2, \cdots$$

中，每个数的素因数都与其它数的素因数互不相同。

注 性质(2)非常重要，由它可以推出“素数是无限多的”。即

因为费尔马数是无限多的，而它们的素因数又彼此不同，所以它实质上又得了素数无限性的另一种证明。

欧拉给出的性质(1)预示着：如果费尔马猜想不成立，即费尔马数中存在合数，它的因数也将是很大的，不易找到。这是对费尔马数问题的最早怀疑。1732年，欧拉终于惊喜地发现：第六个费尔马数F_5有真因数641，

$$F_5=641.6700417。$$

从此费尔马"一贯正确"的幻想被打破了。

1747年欧拉在一篇著作中介绍了他的研究方法。原来欧拉发现了费尔马数的另一个非常重要的性质，即

(3)费尔马数F_n的每一个因数都具有$2^{n+1}\cdot k+1$的形式。这就是说，F_n的所有因数必是等差数列

$$1,\ 2^{n+1}+1,\ 2\cdot 2^{n+1}+1,\ 3\cdot 2^{n+1}+1,\ \cdots$$

中的某些项。当$n=5$时，得到数列

$$1,\ 65,\ 129,\ \cdots,\ 64k+1。\cdots$$

其中第10项为641，恰好整除F_5。

欧拉的工作彻底改变了人们对费尔马数研究的观念，事实上从这里开始人们再也没有找到任何新的费尔马素数，而费尔马合数却如雨后春笋，不断出现。

4．后续的结果

在欧拉证明F_5是合数之后，曾有人试图弥补费尔马猜想的不足。例如，1828年一位匿名者认为：数列

$$2+1,\ 2^2+1,\ 2^{2^2}+1,\ 2^{2^{2^2}}+1,\ \cdots$$

唯一地给出所有的费尔马素数。这是一个错误的猜测，1895年马尔威指出2^8+1不在这个数列中，但它却是素数。后人

还发现$2^{2^{16}}+1$有因数$2^{19}\cdot1575+1=825753601$。

1877年，法国数学家鲁卡斯改进了欧拉给出的性质(3)，指出：

(3′)F_n的每一个因数都是形如$2k\cdot2^{n+1}+1$的数。

这个公式说明：性质(3)中的k只须取偶数就足够了。从而缩减了验算量。例如对于F_5，根据(3′)它的因数必为$2k\cdot2^6+1=128k+1$的形式，此时当$k=6$时就得到了F_5的因数641；而根据(3)却需要$k=10$时才能得到641。即使用(3′)较使用(3)减少了4次验算！

同年，另一位数学家佩平还给出了费尔马数的另一个重要性质：

(4)Fn是素数的充要条件是

$$Fn\mid3^{2^{2^n}-1}+1$$

这一性质对于后人确定费尔马合数发挥了巨大的作用。但是它只能由否定一个数不是素数而证明它是合数，却不能给出它的因数，所以得到许多"知其是合数，却找不到因数"的结果。

还是在这一年的10月，波沃切恩利用鲁卡斯公式找到了另一个费尔马合数F_{12}，它的素因数之一是$7\cdot2^{14}+1=114689$。年底（即两个月后）鲁卡斯也独立地得到了这一结果。又过了两个月（1878年2月），波沃切恩再接再励又证明了F_{23}也是合数，它有素因数$5\cdot2^{25}+1=167772161$。

在短短的几个月中，数学家们一举得到这么多出色的结果，真使人喜出望外。但是仍然存在着令人不安的问题，那就是下一个较小的费尔马数F_6到底是素数还是合数？它的因数

是什么？还始终未得到解决。鲁卡斯曾一再声称：要想求出F_6的因数绝非易事。这件事激怒了一位年已82岁的老人兰德，他在1880年经过几个月的艰苦努力，终于找到了F_6的两个素因数

$$F_6=274177\cdot 67280421310721.$$

兰德老人的精神鼓舞了后人。1895年，数学大师克莱因认为F_7也是合数，1905年，莫尔黑德和韦斯特恩利用佩平公式各自独立地证明了F_7是合数，但是没有找到它的因数。直到1971年，数学家布里哈特和莫里森利用美国加利福尼亚大学洛杉矶分校的一台计算机才找到F_7的两个素因数，即

$$F_7=340282366920938463463374607431768211457$$

$$=59649589127497217\cdot 5704689200685129054721.$$

事实证明，寻找费尔马合数的因数的难易程度不仅取决于F_n的大小，更重要的是看它最小的素因的大小。例如，数字F_7并不很大，但是由于它的两个素因数都比较大，所以为找出它们竟整整经历了80多年的时间。更使人遗憾的是下一个费尔马数F_8，早在1909年莫尔黑德与韦斯特尔就共同证明了它是合数。但是直到1981年，伯恩特和鲍勒德才找到它的一个因数：

$$P=1238926361552897 \mid F_8.$$

然而人们却较早地找到一些大的费尔马数的部分因数。例如，1899年，库尼佛姆找F_{11}的两个因数319489和974849。1903年，外斯顿发现：F_9有因数$2^{16}\cdot 37+1$；F_{18}有因数$2^{22}\cdot 13+1$；F_{12}除有因数$2^{14}\cdot 7+1$（波沃切恩给出的）外，还有因数$2^{16}397+1$和$2^{16}\cdot 7\cdot 139+1$。外斯顿还与库尼佛姆共同发现：其它的费尔马数F_n不存在小于10^6的因数。1906年

莫尔黑德发现F_{73}有素因数$2^{75}\cdot5+1$，等等。

到目前为止，人们已经成功地检验了许多费尔马数，但是始终没有找到新的费尔马素数，却反而找到了50多个费尔马合数。* 这些合数可以分为三类：

第一类，当$n=5,6,7$时，已找到F_n完整的因数分解式。

第二类，当$n=8$，9，10，12，13，15，16，17，18，19，21，23，25，26，27，30，32，36，38，39，42，52，55，58，63，73，77，81，117，125，144，150、207、226，228，250，267，268，284，316，452，1945，3310时，只找到F_n的部分素因数，但是并不知道它们的全部因数。例如。其中的F_{1945}是1957年罗宾逊发现的，他求出F_{1945}的一个素因数$5\cdot2^{1947}+1$。1977年，威廉姆证明了F_{3310}是合数，它的素因数$5\cdot2^{3313}+1$。1980年哥斯汀证明了F_{17}是合数。

注 由于欧拉证明了费尔马合数F_n的因数必为$k\cdot2^n+1$的形式，所以他们从此得到数论界的关注。另外人们还证明了：利用$k\cdot2^n+1$的形式的数字检验费尔马数时，只须用其中的素数试除即可。因此这个问题又成为寻找形如$k\cdot2^n+1$的素数问题。1957年罗宾逊证明了$2^{1947}+1$是素数，它具有586位数字(是F_{1944}的因数)，并且在很长一段时间里一直是这类数字中最大的素数。所以人们为了纪念罗宾逊的贡献，把它们称为罗宾逊数，记为$R(k,n)=k\cdot2^n+1$。1977年威廉姆找到三个更大的逻宾逊素数R(5，3313)、R(5，4687)和R(5,5947)，其中第一个数是F_{3310}的素因数。

---

* 据1975年统计，人们共找到46个费尔马合数。近几年随着计算机的飞速发展，许多新的结果纷纷给出。例如，F_8，F_{17}，F_{3310}等的因数都是新发现的。由于它们不象梅森素数那样“珍稀”，所以很难统计得准确。

第三类，当$n=14$时，仅知道F_n是合数，但没有找到它的任何因数。

另外，当$n=20$，22，24，…时，我们还不知道F_n是素数还是合数。

数学猜想是以部分的事实材料作为立论基础的，它是成功的希望，也有失败的可能。费尔马数猜想就失败了。但是能否引出新的猜想呢？其实数学家们久已推测：大概费尔马数中只有5个素数，而其余的都是合数（如果费尔马在九泉有知，听到这一猜想将会多么伤心！）不过，要想证明这一推测也绝不是一件容易的事，谁知道那一天会不会突然又跳出一个费尔马素数来，！

有些人常为费尔马的失误惋惜：一块光彩照人的美玉竟出现这样的瑕点，真是太遗憾了！且住，现在还不是惋惜的时候。当费尔马数问题在数论中屡受挫之时，另一位数学大师高斯却为它在几何领域赢得一席之地！

5 素数公式介绍

在讲述高斯的工作之前，先插入一段关于素数公式的介绍，这将有助于了解费尔马数猜想产生的历史背景。

前面提到，寻找素数公式是一个十分古老的问题，并且至今仍未得到具有实用性的结果。但是在长期的探索中却发现了许多有价值的数学知识，费尔马数公式就是其中之一。在这里我们概括地介绍一下这方面的工作。

(1) 通过一次函数$f(n)=an+b$是否可以连续地产生素数。这实际上就是求由素数构成的等差数列问题。比如，设$a=2$，$b=3$，则$f(n)=2n+3$。当$n=0$，1，2时，有$f(0)=3$，$f(1)=5$，$f(2)=7$，恰好是一个公差为2的等差数列：3，

5，7。但下一项$f(3)=9$就是合数了。

注 1944年有人证明：存在着无穷多组由三个素数组成的等差数列，但在每组中素数不一定相继。

还有一些好的结果，我们选列如下：

①$f(n)=30n+7$，当$n=0, 1, \cdots, 5$时，得到素数数列：

7，37，67，97，127，157（公差为30）；

②$f(n)=210n+199$，当$n=0, 1, \cdots, 9$时，得到素数数列：

199，409，619，829，1039，1249，1459，1669，1879，2089（公差为210）；

③ $f(n)=223092870n+2236133941$，当$n=0, 1, \cdots, 15$时，给出16个素数。

④ 最出色的结果是1984年由普里切尔德给出的一个公式：

$$f(n)=4180566390n+8297644387,$$

当$n=0, 1, \cdots, 18$时，$f(n)$给出19个素数。这是一个公差为4180566390，首项为8297644387的素数等差数列。

对于数列$\{an+b\}$，1837年数学家狄利克雷证明：当$(a, b)=1$时，$\{an+b\}$中包含无限多个素数。例如，在数列$\{4n+1\}$中，有素数5，13，17，29，37，41，…，因为$(4,1)=1$。在$\{6n+3\}$中只有一个素数，而$\{6n+4\}$中一个素数也没有。

(2) 通过二次函数$f(n)=an^2+bn+c$是否可以连续地产生素数。这个问题最出色的结果是18世纪欧拉给出的，即

$$f(n)=n^2+n+41。$$

它对于80个相继的整数$n=-40, -39, \cdots, 39$均给出素数。但是，当$n=40$时，$f(40)=1681=41^2$不再是素数了。这个公式至今还是由二次函数连续给出素数的冠军。1963年，人们通过高速电子数字计算机(Maniac Ⅱ)检验了由n^2+n+41产生的小于1000万的数字，其中有47.5%是素数。

注 1933年莱赫默证明：形如n^2+n+A ($A>41$)的二次函数，如果$n=0, 1, \cdots, A-2$全给出素数，则A必大于$25\cdot10^7+1$。1934年有人证明，在大数范围内，这样的数最多只有一个。1967年人们证明：没有一个$A>41$能对$n=0, 1\cdots, A-2$使n^2+n+A全给出素数。

有一些结果较好的公式如下：

① $f(n)=n^2-2999n+2224\,8541$，它对于$n=1460, 1461\cdots$。1539也产生80个素数。

② 1798年，勒让得指出：$f(n)=2n^2+29$对于$n=0, 1, \cdots, 28$，可得29个素数。

③ 1983年，数学家乌兰等人发现，公式$f(n)=4n^2+170n+1847$产生的小于10万的数中有46.6%是素数。

④ 乌兰等人还发现，$f(n)=n^2+4n+59$可产生43.7%的素数。

⑤ $f(n)=60n^2-1710n+12150$，当$n=1, 2, \cdots, 20$时，$f(n)+1$与$f(n)-1$是一对素数(其中有一对负值-29与-31)。

但是，不管结果多么好，实际上人们已经证明：不存在可以唯一产生素数的整系数多项式。

证明 设多项式

$$f(x)=a_kx^k+a_{k-1}x^{k-1}+\cdots+a_0$$

(其中a_k是整数)，对于x的所有整数值都给出素数。则当

$x=m$时，设上式得到素数p，即

$$p=a_k m^k+a_{k-1}m^{k-1}+\cdots+a_0,$$

现取$x=m+np$，则我们必然可得到另一个素数设为q，且有

$$q=a_k(m+np)^k+a_{k-1}(m+np)^{k-1}+\cdots+a_0.$$

这里　$a_k(m+np)^k=a_k m^k+$（包含p的项），

$a_{k-1}(m+np)^{k-1}=a_{k-1}m^{k-1}+$（包含$p$的项），

……

等等，所以

$$Q=a_k m^k+a_{k-1}m^{k-1}+\cdots+a_0+(\text{包含}p\text{的项})$$

$$=p+(\text{包含}p\text{的项}).$$

虽然该式子可被p整除，即$p\mid Q$。这与Q是素数矛盾。所以不存在可以唯一产生素数的多项式。

注　相反地人们却证明：有无限多个整数x使多项式$f(x)$是合数。

（3）　存在一个实数θ，它使

$$f(n)=[\theta^{3^n}]$$

对所有的n都为素数。其中$[x]$表示不大于x的整数。

注　这个公式是穆尔士给出的。表面上看它似乎解决了素数公式问题，实际上要想确定θ，需要识别任意大的素数，还是不可能的。若可能的话，我们既然已经识别了任意大的素数，还要此公式何用？

（4）　1961年塔尔曼给出一个公式：

$$p=\frac{P_n}{p_i p_k\cdots p_n}\pm(p_i p_k\cdots p_n),$$

其中P_n是前n个素数p_1，p_2，…，p_n之积，p_i，p_k，…，p_n是前n个素数中的任意几个互异素数（也可以是全部）。则

如果p是比第$n+1$个素数的平方小的数，它就是素数。

例如，

$$p=\frac{2\cdot3\cdot5\cdot7\cdot11\cdot13\cdot17\cdot19\cdot23}{2\cdot3\cdot11\cdot13\cdot17}-(2\cdot3\cdot11\cdot13\cdot17)$$

$$=709,$$

因为$709<29^2$，所以它是素数。

(5) 函数

$$f(x,y)=\frac{y-1}{2}[|B^2-1|-(B^2-1)]+2,$$

其中$B=x(y+1)-(y!+1)$，则当x和y都取正整数时，它唯一地产生所有的素数，并且每个奇素数值正好各取一次。

§5.2 高斯公式

自从1732年欧拉用反例否定了“费尔马数猜想”之后，这个问题突然名声大振，因为他毕竟是“数论之父”犯下的错误。许多人都认为它失去了数学价值，只能作为一个教训警示后人。但是，当另一位数学大师高斯接手这个问题之后，费尔马数再度闪烁出夺目的光彩。这里有一段非常动人的故事。

那是在1796年，19岁的高斯正在德国哥廷根大学读书。他勤奋好学，聪颖过人，在拉丁文、数学等许多方面都有较深的造诣，他正处在选择学科的“十字路口”。一天，在研究几何学时他发现：在欧几里得时期，人们就用圆规和直尺完成了正三边形、正四边形、正五边形，以及由此推演出的

正六边形、正八边形、正十边形等等的作图法。但是，2000多年过去了，竟然没有人能用圆规和直尺作出正七边形、正九边形和正十一边形等图形。这是为什么？前人没有给出答案。高斯向他的导师求教，导师却劝他退避三舍，莫为此空耗青春。这更激发了高斯强烈的求知欲望和对数学的浓厚兴趣。

首先，高斯从正多边形的边数入手，他很快就发现，迄今已用圆规和直尺作出的正多边形的边数可归结为下述几种：$2^n(n=2,3,\cdots)$和$2^n\cdot 3$，$2^n\cdot 5$，$2^n\cdot 15(n=1,2,\cdots)$。这里有什么规律呢？高斯的天才就在于能从繁杂的现象中迅速地摸到事物本质（比如，他在10岁时就发现了自然数求和规律，很快地求出了$1+2+\cdots+100=101\times 50=5050$，使老师大吃一惊）。果然他总结出，上述边数中只出现了素数2、3和5和它们的乘积（如$3\times 5=15$等）。于是他采取类推法判断：大概是以某些特殊的素数或它们的乘积为边数的正多边形可以用圆规和直尺作图。然而7是素数，为什么正七边形作图却百思而不得其解呢？这时，高斯感到了几何知识的局限性，他越出几何学的范畴，对数论进行了认真的研究。偶然间他惊喜地发现，3和5恰好是费尔马数F_0和F_1。高斯迅速地紧缩了他的研究范围：再次推断：大概以费尔马素数为边数的正多边形可以用圆规和直尺完成。于是他越过素数7、9和11，开始致力于下一个费尔马素数$F_2=17$为边数的正17边形的作图。果然，高斯成功了！他用圆规和直尺完成了正17边形的作图。请看下面的作图过程：

作法　在图5-1中作一个半圆，圆心为O，半径为OA，再作一个垂直于OA的半径OB、在OB上取一点C，使OC等于

$\frac{1}{4}OB$。作$\angle OCD=\frac{1}{4}\angle OCA$，并且$\angle ECD=45°$。以$EA$为直径作一个半圆交$OB$于$F$。以$D$为圆心，$DF$为半径再作一

图5-1

个半圆交OA所在直径于H和G，过G和H作垂线，交大圆于P和Q，则P和Q是等于圆周长的2/17的一段弧的两个端点。这段弧的分点是R，则PR或RQ就是正十七边形的边长。

接着，高斯又天才地把几何问题同代数问题结合起来，开创了所谓“分圆问题”的研究。我们知道，求作正多边形与等分圆周问题是等价的。即只要你能用圆规和直尺将一个圆周分成几等分，就能作出相应的正多边形；反之亦然。而方程$Z^n=1$的n个根正好是复平面上以原点为中心，以1为半径的单位圆周上的n个等分点所表示的复数值。高斯想到了这一点，并且认真地研究了方程$Z^n-1=0$（现称分圆方程）的复数根的情况。得到结论：当方程$Z^n-1=0$的复数根的实部和虚部的数量可以用圆规和直尺作出时，圆周的n分之一也就可以作出来。从而这个n边形也可以作出来。

那么，什么样的数量可用圆规和直尺作出来呢？运用几何学知识很容易证明：凡是由有理数通过加、减、乘、除、

开方等五种规则运算经有限多次得出来的数量（用线段长度表示的量），均可由圆规和直尺作图法作出来。所以，一个正 n 边形能否用圆规和直尺作出来，关键是看方程 $Z^n-1=0$ 的复数根的实部和虚部的数量是否是由加、减、乘、除、开方等五种规则运算构成的。例如，$Z^3-1=0$ 的三个根是

$$Z_1=1,$$

$$Z_2=-\frac{1}{2}+\sqrt{\frac{\ }{1}}\,i$$

$$Z_3=Z_2^2-\frac{1}{2}-\sqrt{\frac{3}{2}}\,i,$$

它们的实部和虚部显然是由上述五种运算构成的，所以正三边形可以用圆规和直尺作出来。

再如，$Z^5-1=0$ 的五个根是

$$Z_1=1,$$

$$Z_{2,3,4,5}=\frac{1}{2}\left\{\left(\frac{-1\pm\sqrt{5}}{2}\right)\pm i\sqrt{4-\left(\frac{-1\pm\sqrt{5}}{5}\right)^2}\right\},$$

也符合上述条件，所以正五边形也可以用规尺作出来。

高斯运用他坚实的数学基础和娴熟的计算技巧求解了以第三个费尔马素数 $F_3=17$ 为指数的方程 $Z^{17}-1=0$，结果得到了它的17个根：

$$Z_1=1,$$

$$Z_2=1/2\cdot(W+\sqrt{W^2-4}),$$

$$Z_3=Z^{-1}_2=1/2\cdot(W-\sqrt{W^2-4}),$$

其余的分点可由 Z_2^k（$k=\pm2,\ \pm3,\ \cdots,\ \pm8$。）表出。其中

$$W=\frac{1}{8}(\sqrt{17}-1+\sqrt{34-2\sqrt{17}})+$$

$$\frac{1}{8}\sqrt{(\sqrt{17}-1+\sqrt{34-2\sqrt{17}})^2+16(\sqrt{17}+1-\sqrt{34+2\sqrt{17}})}。$$

这个根数完全是由和、差、乘、除、开方表示出来的，由此证明了正十七边形作图的可行性。

高斯完成上述工作恰好是在1796年3月30日，(他还差一个月满19岁)！伟大的成功使他惊喜无比，兴冲冲地跑到著名教授数学家克斯特纳那里说："我作出了正十七边形"。教授哑然失笑，他连看也不看，并轻视地说他定错无疑！高斯反驳道他已经用降次法解出了17次二项方程．并且由此给出了正十七边形作图可能性的证明．克斯特纳认为高斯是在梦呓，并嘲笑地说："噢，好，我已经这样作了"．

正十七边形作图的成功，坚定了高斯从事数学研究的决心，他著名的《数学日记》就从这一天(1796年3月30日)开始动笔了。这本日记中包括146个条目，最后一条的日期是1814年7月9日。它的全文采用了密码式文字书写，例如，1796年7月10日记载：

$$\text{EYPHKA!}\quad num=\Delta+\Delta+\Delta,$$

它表示"每个正整数是三个三角形数之和！"至今还有两条没有被破译。由于高斯不愿轻意展视自己的发现，直至1898年人们才见到这本日记。

在正十七边形作图的基础上，高斯还给出一个重要定理：

高斯定理 从一个正多边形可以用圆规和直尺作图的充要条件是它的边数等于

$$2^l\cdot p_1\cdot p_2\cdots p_n,$$

这里p_1，p_2，…，p_n是形如$2^{2^k}+1$的费尔马素数，l为任何

正整数或零。

高斯仅给出这一定理充分性的证明，而必要性证明是1837年由温泽尔给出的。所以又称为“高斯-温泽尔定理”。1800年，高斯将“分圆方程”的有关工作收入名著《算术研究》的最后一节之中，并寄给巴黎科学院。也许是此书过于深奥或作者过于年轻（23岁），科学院拒绝接受这部论著，但高斯自己发表了。事实证明：《算术研究》是一部划时代的不朽之作。

许多年过去了，高斯在数学领域中建立了许多丰碑，这使他荣获“数学家之王”等美誉。正十七边形“为他诱发的数学灵感仍使他终生难忘。因此他留下遗言：“我死后，请后人在我的墓碑上刻上正十七边形”。虽然后人没有满足他的愿望，但是在高斯故乡布鲁斯维克确实为他建立了一个刻有正十七边形的纪念碑。

还有一个重要问题，就是至今人们才找到5个费尔马素数：$F_0=3$，$F_1=5$，$F_2=17$，$F_3=257$和$F_4=65537$，还不知道是否存在更大的费尔马素数。并且高斯也没有给出更大的正多边形的作法，却巧妙地证明了费尔马素数的可作图性。这也是一个“非构造性证明”（就象本书第三章中提到的“证明了某数是合数，却找不到它的因数”一样）。所以有些人怀疑高斯定理的正确性，希望在有限的范围内检验它的真伪。1832年，德国数学家黎西罗不畏艰辛，成功地用规尺作出了以第四个费尔马素数为边长的正257边形；继而，林根与赫姆斯用10年时间作出了正65537边形，仅手稿就有一大箱子，至今保存在哥廷根大学。

回顾这段曲折的历程，人们可以从中得到一条重要的启

示：不要轻信世人对伟人的肆意评说（现在流行的说法认为费尔马的推测太随便了），而应当细细领会他们当时的思想过程，那很可能是成功的契机（高斯不就是由费尔马数而获益的吗？）也不要轻信伟人的预言，世界是一个五光十色的万花筒，谁也无法预测到它的全部图案！

第六章 伪 素 数

当我们不能用数学指南针或经验的火炬时，…肯定的，我们连一步也不能向前迈进。

——伏尔泰

§6.1 费尔马小定理的逆定理

对于一个合数n，如果它整除2^n-2，即

$$n \mid (2^n-2),$$

则n就称为伪素数。例如，人们已经证明：$341=11\cdot 31$是合数，并且它能够整除$2^{341}-2$，所以341是一个伪素数。读者会问：明明是合数，为什么具有这一性质就与素数联系起来了呢？这里包含着一个非常奇妙的故事。

1.费尔马小定理

本书第三章曾提到，1640年6月费尔马在致梅森的一封信中给出了数论中的三个重要性质，其中的第2个性质是：如果n是素数，则$2n \mid (2^n-2)$。同年10月，费尔马在致福兰尼克尔的一封信中给出了它的一般性叙述，即

费尔马小定理● 如果p是任意整数，并且a是任意不能被p整除的整数，则

$$p \mid (a^{p-1}-1).$$

证明 可以证明，$p \mid a^{p-1}-1$等价于$p \mid a^{p}-a$，所以我们仅给出这个等价形式的证明。

用数学归纳法。当$a=1$时，定理显然成立。

设当a是大于1的某一个正整数时，$p \mid (a^{p}-a)$，往证定理对于$a+1$也成立。即证

$$p \mid [(a+1)^{p}-(a+1)].$$

由二项式定理有

$$(a+1)^{p}=a^{p}+C_{p}^{1}a^{p-1}+\cdots+C_{p}^{p-1}a+1,$$

移项得

$$(a+1)^{p}-a^{p}-1=C_{p}^{1}a^{p-1}+\cdots+C_{p}^{p-1}a.$$

可以证明$p \mid C_{p}^{k}$（$k=1, 2, \cdots, p-1$），所以

$$p \mid [(a+1)^{p}-a^{p}-1].$$

又根据归纳假设$p \mid (a^{p}-a)$，得

$$p \mid [(a+1)^{p}-a^{p}-1+(a^{p}-a)],$$

而右端即是$(a+1)^{p}-(a+1)$。所证成立。

对于负值的情况，不妨记为$-a$，a是正整数。如果p等于2，则有

$$(-a)^{p}-(-a)=(-a)^{2}-(-a)=a(a+1).$$

因为a和$(a+1)$是两个相邻正整数，必一个是奇数，一个是偶数，所以它们的乘积可被2整除。如果p的奇素数，则有

● 这种，小定理”的叫法是与费尔马的另一个定理相对应的，即“当$n>2$时，$x^{n}+y^{n}=z^{n}$没有正整数解”。世称“费尔马大定理”，或“费尔马最后定理”（因为它至今还没能解决）。关于它的介绍见本书第七章勾股数。

$$(-a)^p-(-a)=-a^p+a=-(a^p-a),$$

根据前面的证明已知$p\mid(a^p-a)$，所以p也整除$-a(a^p-a)$。

注 费尔马在提出这个定理时，没有给出证明1683年 莱布尼兹曾宣称给出了它的证明，但无人见到。上述完整的证明结果是1736年欧拉给出的。

费尔马小定理产生之后，人们自然会想到它的逆定理是否成立。就是说，如果$n\mid(a^n-a)$，则n是否一定为素数？据考证，在费尔马时代人们默认了n一定是素数，起码认为n整除$2-2$（即$a=2$）时，n一定是素数。例如，在本书第五章费尔马数中，曾提到费尔马推测$F_n=2^{2^n}+1$是素数。他的依据大概就是因为"每一个F_n都整除$2^{F_n}-2$"。这个证明并不困难：

根据费尔马小定理，当$n=0$，1，…，4时，因为F_n是素数，所以$F_n\mid(2^{F_n}-2)$。现在考虑$n>4$的情况。由于$n+1<2^n$，所以2^{n+1}整除2^{2^n}，于是存在一个正整数k，使得$2^{2^n}=2^{n+1}\cdot k$，所以有

$$\begin{aligned}2F^n-2&=2\left[(2^{2^{n+1}})^k-1^k\right]\\&=2\left[(2^{2^{n+1}}-1)(\cdots)\right]\\&=2(2^{2^n}+1)(2^{2^n}-1)(\cdots)\\&=2F_n(2^{2^n}-1)(\cdots).\end{aligned}$$

显然上式可以被F_n整除。因为当时费尔马还不知道存在伪素数，也就是说他认为费尔马小定理的逆定理也成立，所以才断言F_n一定是素数。

1680年6月与1681年12月，著名科学家莱布尼兹曾两次明确宣称，自己证明了：如果n不是素数，则2^n-2不能被n整除。1742年4月，哥德巴赫在致欧拉的一封信中也试图证明费尔马小定理的逆定理成立，但是都没有成功。从费尔马提出"小定理"时起（1640年），这个"伪素数"的悬案竟整整延续了近200年之久。

2.匿名者的发现

1830年，一位不愿意公布姓名的德国人宣称：他否定了费尔马小定理的逆定理，即"当n为合数时，$a^{n-1}-1$也可能被n整除"。他证明的大意是：在$a^{p-1}=kp+1$中（p为素数），设$k=\lambda q$，则pq整除$(a^{(p-1)q}-1)$。因此，如果pq整除$a^{q-1}-1$，则pq整除$a^{pq-1}-1$，由此可推出$q-1$是$p-1$的倍数。他还举出一个例子：如果$p=11$，$q=31$，$a=2$，则341整除$2^{341}-2$。现在给出推导过程：

$$
\begin{aligned}
2^{341}-2=2(2^{340}-1)&=2\left[\left(2^{10}\right)^{34}-1^{34}\right]\\
&=2(2^{10}-1)(\cdots)\\
&=2\cdot 1023(\cdots)\\
&=2\cdot 3\cdot 341(\cdots),
\end{aligned}
$$

所以341整除$2^{341}-2$。这就是人们发现的第一个既整除2^n-2，又不是素数的数。因为它把人们欺骗的时间太长了。所以被命名为"伪素数"，或"假素数"。

注 在当时的欧洲有一种风气，就是给出惊人的结果而不公布姓名。再如本书第一章中提到的发现第5个完全数的学者（1640年）也没有公布姓名。其原因大概是为了增加问题的神秘感，或是怕暴露身份，引来是非。

第二个伪素数是1876年由鲁卡斯发现的，即2701＝

$37\cdot73$整除$2^{2701}-2$.1899年,杰恩斯一举给出了4个伪素数:

$$1387=19\cdot73,\quad 4369=17\cdot257$$

$$4681=31\cdot151,\quad 10261=31\cdot331。$$

他使用的方法是:如果$p\mid2^q-2$,且$q\mid2^p-2$,则$pq\mid2^{pq}-2$。1909年,巴纳切维斯基证明了:对于$n<2000$可以整除2^n-2的合数n只有

$$341=11\cdot31,\quad 561=3\cdot11\cdot17,$$

$$1387=19\cdot73,\quad 1729=7\cdot13\cdot19$$

$$1905=3\cdot5\cdot127。$$

从上述结果中可以发现,早年人们找到的伪素数都是奇数。1926年,数学家普勒发表了到5亿为止的全部奇数伪素数;1938年,他又把这个结果扩充到十亿之内。因此,伪素数又有普勒数之称。数学家们还证明了:存在着无限多个奇数伪素数。这一结论得到的十分巧妙,是下述定理的一个推论。

定理 如果n是大于1的奇数伪素数,则2^n-1也是奇数伪素数。

证明 因为n是奇合数,所以存在一对大于1的奇数a、b,使得$n=ab$,于是

$$\begin{aligned}2^n-1&=2^{ab}-1=(2^a)^b-1^b\\&=(2^a-1)(\cdots),\end{aligned}$$

显然$2^a-1\neq1$(否则有$a=1$,矛盾)且$2^a-1\neq2^n-1$(否则有$b=1$,亦矛盾),所以2^n-1是合数。又因为n是伪素数,所以它整除2^n-2,即存在一个正整数k,使$2^n-2=nk$,于是有

$$2^{2^n-2}-1=2^{nk}-1=(2^n)^k-1^k$$

$$=(2^n-1)(\cdots)。$$

所以2^n一整1除$2^{2n-2}-1$，因此也整除$2^{2n-2}-2$。所以2^n-1是伪素数。

根据这一定理自然可以推出：从任一个奇数伪素数出发，都可以得到无限多个奇数伪素数。所以得到结论：奇数伪素数是无限多的。

3. 奇异的性质

(1) 偶数伪素数：在完善奇数伪素数问题的同时，人们一直关注着偶数伪素数的研究。很长一段时间里，人们一直没有找到它们。直至1950年才由莱赫默给出了第一个偶数伪素数$161038=2\cdot73\cdot1103$，即

$$161038 \mid 2^{161038}-2。$$

它的证明并不困难（但找出它去

$2^{161038}-2$分解：

$$2(2^{161037}-1)=2(2^9-1)(\cdots)$$
$$=2(2^{29}-1)(\cdots),$$

而$73\mid(2^9-1)$，$1103\mid(2^{29}-1)$，所以可推出161038是伪素数。

翌年，荷兰数学家比格尔证明了：偶数伪素数也是无限多的。

(2) 绝对伪素数：如果合数$n\mid(a^n-a)$，对于$a=1,2,\cdots$均成立，n就称为绝对伪素数。这类数字是1909年由数学家卡迈克尔开始研究的，因此又称为卡迈克尔数。可以证明，$561=3\cdot11\cdot17$是一个绝对伪素数（而且是最小的一个）。为了说明这一点，只须证明561的素因数3、11和17均整除$a^{561}-a$。我们有

$$a^{561}-a=a\left[(a^2)^{280}-1^{280}\right]$$
$$=a(a^2-1)(\cdots)$$
$$=(a^3-a)(\cdots),$$

根据费尔马小定理知$3\mid(a^3-a)$，所以$3\mid(a^{561}-a)$。又由

$$a^{561}-a=a\left[(a^{10})^{56}-1^{56}\right]=a(a^{10}-1)(\cdots)$$
$$=(a^{11}-a)(\cdots),$$

同上可证$11\mid(a^{561}-a)$。再由

$$a^{561}-a=a\left[(a^{16})^{35}-1^{35}\right]$$
$$=a(a^{16}-1)(\cdots)$$
$$=(a^{17}-a)(\cdots),$$

可证$17\mid(a^{561}-a)$。所以561是绝对伪素数。

另外几个绝对伪素数是：

$2821=7\cdot13\cdot31$，

$10585=5\cdot29\cdot73$，

$15841=7\cdot31\cdot73$。

它的确定工作比较困难，直到1978年人们才找到685个绝对伪素数，其中最大的一个是

$$443656337893445593609056001$$
$$=11\cdot29\cdot31\cdot37\cdot41\cdot43\cdot61\cdot71\cdot73\cdot79\cdot97\cdot113\cdot127\cdot131\cdot151。$$

但是，到目前为止，人们还没能证明是否存在着无限多的绝对伪素数。

（3）超伪素数：我们知道，伪素数又有普勒数之称，当伪素数的所有因数d都满足关系式$d\mid(2^d-2)$时，就称之为超普勒数或超伪素数。例如，$2047=23\cdot89$，它不但是一个伪素数，而且也是一个超伪素数。说明这一点并不困难：根

据费尔马小定理，因为23和89都是素数，所以有$23 \mid (2^{23}-2)$与$89 \mid (2^{89}-2)$成立。从这个例子中显然可以得出结论：仅有两个素因数的伪素数，或者它的合数因数也是伪素数的伪素数，必是超伪素数。并非所有的伪素数都是超伪素数，例如$561=3\cdot11\cdot17$就不是超伪素数，因为可以证明：33不能整除$3^{33}-2$。

人们已经证明：①存在无限多个超伪素数。这一结果是1936年莱赫默给出的，他首先证明了存在无限多个只有两个素因数的伪素数，而这样的伪素数都是超伪素数，所以超伪素数是无限多的。②所有的超伪素数都是奇数。现证明如下：假如$2n$是超伪素数，则有$2n \mid (2^{2n}-2)$，且对于$2n$的因数n也有$n \mid (2^n-2)$。将前式两端除以2得$n \mid (2^{2n-1}-1)$，显然n是奇数。因此由$n \mid 2(2^{n-1}-1)$可得$n \mid (2^{n-1}-1)$.从而有

$$n \mid [(2^{2n-1}-1)-(2^{n-1}-1)]，即$$

$$n \mid 2^{n-1}(2^n-1).$$

由于n是奇数，所以$n \mid (2^n-1)$.又因为$n \mid (2^n-2)$，所以只有$n=1$，$2n=2$.根据超伪素数必是伪素数，而伪素数必是合数的定义，矛盾。所以不存在偶数超伪素数。

4. 数学地位

从否定费尔马小定理的逆定理开始，人们陆续发现了许多的伪素数.并且至今仍对这个问题兴致勃勃.其原因何在呢？原来这又涉及到当前数论研究的一个热门：确定素数问题.在前几章中我们多次提到，在漫无边际的自然数中要想确定一个大数的性质.简直比登天还难。近年来数学家们认为，用费尔马小定理确定素数也是一种有效的办法.设n是一个需要鉴定的大数，用n试除2^n-2.如果除不尽，则n一定是

合数；如果除尽了，则n有很大可能是素数（也可能是伪素数）。但是，这个可能究竟有多大呢？据统计，在10^{10}之内素数有455052512个，而伪素数只有14884个。这就是说，如果$n\mid(2^n-2)$，则n有99.9967%的可能是素数。这样一来，问题发生了本质的变化：从前是在大量的合数中筛出素数来，现在却是从大量的素数之中筛去寥寥无几的伪素数了。显然，在这项工作中如何准确快速地确定伪素数是至关重要的！这也正是当代数学家们"喜爱"伪素数的原因所在。1982年，《美国科学新闻》第27期的封面上赫然写着：

561

PRIME OR NOT PRIME?

即"561，是否为素数"（它是伪素数）。这期杂志中介绍了利用伪素数的性质检验素数的算法，并指出：在这种算法产生之前，要检验一个百位数字，一般需要100多年。有了这种算法，仅需15秒钟；据了解，经适当调整后，仅需5秒钟。

§6.2 "中国定理"之谜

众所周知，我国有着悠久的数学研究的历史。我们的祖先曾创立了许多重要的数学理论，它是我国古代文化的一个重要组成部分。现代数学史学家们经过长期和大量的考证后发现，许多重要的数学成就都可以在中国古算书中找到思想根源或萌芽。但是，近代西方却流行一种说法，认为：

早在孔子时代（约2500多年前），中国人就已经知道了费尔马小定理的特殊形式：如果n是素数，则$n\mid(2^n-2)$。

并且，中国人还认为费尔马小定理的逆定理："如果$n \mid (2^n-2)$，则n是素数"也成立，因此命名为"中国定理"。恰恰因为这个逆定理不成立，并且由此产生了伪素数，所以"中国古人给出了一个错误定理"的说法就更为引人注目了。

近年来，随着西方众多数学史读物的传入，我国的一些人也尾随这个观点。这究竟是怎么一回事呢？遍览我国许多优秀的数学史论著，却连这方面的一点介绍也没有。那么，这些西方人的观点依据又是什么呢？

人们知道，在当代西方研究中国科学技术史的泰斗当属英国剑桥大学李约瑟。对于所谓"中国定理"问题，李约瑟进行了细致确凿的考证，结果发现了谬误的根源。原来这种说法最早出现在1897年数学家杰恩斯的一篇短文之中。当时杰恩斯还是一个大学生，他在这篇短文的附注中奇怪地写道：

威托马爵士的一篇论文中认为，在孔子时代就已有了这个定理（指费尔马小定理），并且（错误地）说，如果p不是素数，则此定理不成立。

后来，著名的数学史专家迪克森在名著《数论史》中也讲述了这种观点，从而流传开来。

李约瑟认为：杰恩斯等人的观点是由于西方汉学家对中国著名古算书《九章算术》的一些错误理解所致。据悉早期的西方汉学家搞不清《九章算术》的成书年代，而孔子在西方却非常著名，许多学者都习惯把中国某些古代发明笼统地说是在孔子时代。所以杰恩斯等人误称《九章算术》成书于孔子时代是不足为奇的。

注　实际上我国《九章算术》约成书于公元前1世纪。

在进一步的考证中李约瑟认为，杰恩斯等人在解释《九章算术》中关于“偶数能被2除尽，而奇数则不能”这一叙述时发生了误解。《九章算术》方田章中写道：“可半者半之。不可半者副置分母子之数，以少减多，更相减损。求其等也”．它的实际意思是：如果分子和分母都可为2除尽，则分子、分母都折半．如果分子和分母不能为2除尽，则分别对分子和分母设定某些数，不断辗转地从大数中减去小数．并求出它们的相等值，即继续进行到最后的被减数等于最后的减数为止．这实际上是用辗转相除法求最大公约数的一个法则。但是，杰恩斯等人没有正确地弄懂这段话，而想到了 $\frac{x^{2-1}-1}{2}$，便把第一句话理解为以2作分母，接着就大谈其从大数减去小数了。他们可能把“更”字解释成“再”字，以适应第二项－1。但是其余的，他们就无法翻译了。李约瑟指出：杰恩斯等人这种的解释完全不符合《九章算术》的原义。毫无疑问，中国汉代的数学家绝不会想到任意数x就是x^{2-1}。”

伪素数的故事再次告诉我们一个真理：严格的逻辑论证是数学研究的生命线和指南针，离开它任何人都会一事无成。正如大数学家海维赛德的一句名言：逻辑可以等待，因为它是永恒的。

第七章　勾　股　数

在大多数科学里，……只有数学，每一代人都能在旧建筑上增添一层楼。

——汉克尔

§7.1　悠久的历史

对于正整数a、b和c，如果存在关系

$$a^2+b^2=c^2,$$

则a、b和c称为勾股数组，一般记为(a, b, c)。其中的数字称为勾股数。例如，3，4和5就存在关系$3^2+4^2=5^2$，所以它们是一组勾股数。这个名称来源于我国公元前1世纪的古算书《周髀算经》，书中记载了约公元前11世纪商高与周公的一段对话，其中写道："故折矩，以为勾广三，股修四，径隅五"。这里的"勾"是指直角三角形较短的直角边，"股"是指另一条直角边，"径"是指斜边。实际上商高指出：作一个直角三角形，如果短直角边（勾）是3，长直角边（股）是4，那么斜边（径）就是5。这便给出了一组所谓"勾股数"。《周髀算经》中还载有陈子与荣方的一段对话，陈子说："若求邪至日，以日下为勾，日高为股，勾、股各自乘，并而开方除之，得邪至日。"这是一个"测量日

高"的应用问题，若把它的数学内涵抽象出来，即是：把一个直角三角形的直角边长（设为x、y）分别平方后相加，再开平方，就得到了斜边长（设为z）。所以说，陈子得到了直角三角形三边之间的一般关系：

$$x^2+y^2=z^2.$$

这就是著名的勾股定理。当式中的x、y和z均为正整数时，显然是一组勾股数。因此，"勾股数"这一名字正是产生于直角三角形三边之间的重要联系之中。

人类发现勾股定理是一件了不起的大事，而与这一发现密切相关的勾股数也在数学史中占有重要地位。人们已经证实：在四大文明古国——中国、埃及、印度和巴比伦的史册上均有勾股数的记载。例如，古埃及人早在公元前23世纪就给出了数组（3，4，5），并于公元前5世纪给出（5，12，13），（7，24，25），（8，15，17）和（12，35，37）。

最惊人的结果是1945年发现的一份古巴比伦人的数学手稿，它刻在一块汉穆拉比时代的泥板上，约成文于公元前1900年至公元前1600年间，现存于美国哥伦比亚大学中。在这份手稿中刻有15组勾股数，是用60进位制数记录的，译成印度-阿拉伯数字后，用逗号分开它们的位数，就得到了表7·1。

注 所谓60进位制记数就是"逢60进1"。将表7·1中的60进位制数转换成10进位制数很容易。例如，第一组数：

$$a=(2,0)_{60}=(2\times60+0)_{10}=120,$$

$$b=(1,59)_{60}=(1\times60+59)_{10}=60+59=119,$$

$$c=(2,49)_{60}=(2\times60+49)_{10}=120+49=169.$$

由于古巴比伦人没有"零"号，很长时间人们无法弄清

表7·1　　古巴比伦人记载的勾股数表

	a	b	c
1	2,0	1,59	2,49
2	25,36	56,7	1,20,25
3	1,20,0	1,16,41	1,50,49
4	3,45,0	3,31,49	5,9,1
5	1,12	1,5	1,37
6	6,0	5,19	8,1
7	16,0	13,19	20,49
8	10,0	8,1	12,49
9	1,48,0	1,22,41	2,16,1
10	1,0	45	1,15
11	45,0	38,11	59,1
12	40,0	27,59	48,49
13	4,0	2,41	4,49
14	45,0	29,31	53,49
15	1,30	56	1,46

它们的位数，因此迟迟未能译出结果。按照表7·1中的“断位”方法就得到了15组惊人的勾股数：

1. 119，120，169；

2. 3367，3456，4825；

3. 4601，4800，6649；

4. 12709，13500，18541；

5. 65，72，97；

6. 319，360，481；

7. 2291，2700，3541；

8. 799，960，1249；

9. 481，600，769；

10. 4961，6480，8161；

11. 45, 60, 75;

12. 1679, 2400, 2929;

13. 161, 240, 289;

14. 1771, 2700, 3229;

15. 56, 90, 106。

另外，古印度人也曾给出一些勾股数，最早的记载见于公元前5世纪的宗教建筑规范“绳子的规则”。其中给出了6组勾股数，它们可以分为三类：

表7·2　　古印度人给出的勾股数表

$b-c=1$	$b-c=2$	$b-c=3$
3, 4, 5	8, 15, 17	15, 36, 39
5, 12, 13	12, 35, 37	
7, 24, 25		

中国对于勾股数的贡献是非凡的。除了著名的《周髀算经》中的记载之外，另一部举世闻名的古算书《九章算术》（约成书于公元前1世纪）以专章介绍了勾股定理的性质和应用，并且给出了几组勾股数（3，4，5），（5，12，13），（7，24，25），（8，15，17）和（20，21，29）。

但是，关于勾股定理和勾股数最丰富的研究是在古希腊时期。大约在公元前500年，著名的毕达哥拉斯学派首先给出了勾股定理的严格证明。后来他的证法失传了，现存的最早证法见于欧几里得的《几何原本》之中。另外，毕达哥拉斯以及柏拉图（约公元前400年）和欧几里得分别给出了勾股数的三个性质，现叙述如下：

毕达哥拉斯公式　设

$$a=2n+1,$$

$$b=2n^2+n,$$
$$c=2n^2+n+1,$$
则当n取正整数时，(a, b, c)是一组勾股数。

注 毕达哥拉斯给出的勾股数公式不能表示所有的勾股数，只能表示$c-b=1$（即直角三角形的弦与一个直角边的差等于1）的那一类数组。后面的柏拉图公式和欧几里得公式也只能给出一些特殊的勾股数组。另外，鉴于毕达哥拉斯学派的伟大贡献，现在世界上普遍把勾股定理和勾股数称为毕达哥拉斯定理和毕达哥拉斯数。

柏拉图公式　设
$$a=2n,$$
$$b=n^2+1,$$
$$c=n^2-1,$$
则当n取正整数时，它表示$c-b=2$的那一类勾股数。

欧几里得公式　设
$$a=\alpha\beta\gamma$$
$$b=\frac{1}{2}\alpha(\beta^2-\gamma^2),$$
$$c=\frac{1}{2}\alpha(\beta^2+\gamma^2),$$
则当α，β和γ取正整数，且$\beta>\gamma$时，它也表示一组勾股数。如果设$m=\alpha\beta^2$，$n=\alpha\gamma^2$，则可以得到欧几里得公式的等价形式：
$$a=\sqrt{mn},$$
$$b=\frac{1}{2}(m-n),$$
$$c=\frac{1}{2}(m+n),$$
其中m、n具有相同的奇偶性，并且$m\cdot n$是完全平方数。

以上三位大师的工作不但揭示出勾股数的内在规律性，而且充分体现了古希腊学者高超的数学水平。

由于勾股数的"故乡"遍布在各个古老的文明国度里，所以许多年来一些国家总为勾股定理的发现权问题争论不休，并且使它得到了各种不同的命名。例如，商高定理，陈子定理，毕达哥拉斯定理，百牛定理*，以及将（3，4，5）称为商高数，埃及数，将以3：4：5为边的直角三角形称为商高三角形，埃及三角形，等等。可以推测，在古希腊之前，古巴比伦、印度、埃及和中国的先贤们都可能发现了勾股定理的证明，但是岁月的风尘淹没了许许多多的历史真相，使后人无从寻觅，只有遵循已知的历史事实来说明历史（现在世界上把勾股定理称为毕达哥拉斯定理的人最多）。当然，用什么来命名并不是问题的关键，无论是谁最早发现的勾股定理，它都是全人类的财富。

§7.2 有趣的性质

勾股数的有趣性质不仅仅体现在与直角三角形的一般关系上，它自身也包含着许多知识。

1．基本性质

首先，我们很容易证明：勾股数组是无限多的。比如，设（a，b，c）是一组勾股数，显然（ka，kb，kc）也是一组勾股数，而当$k=1$，2，…时，就得到了无穷多组勾股数。一般讨论勾股数的性质时，都从基本勾股数组入手，即如果勾股数a、b和c两两互素，就称之为一组基本勾股数**。

---

* 相传毕达哥拉斯学派曾为得到了勾股定理的证明而欢喜若狂，为此他们杀了一百头牛祭神。所以勾股定理又有"百牛定理"之称。

** 实际上，只要（a，b）＝1，就可以推出a、b和c两两互素。

下面我们介绍一下基本勾股数组的几个性质：

（1）在基本勾股数（a，b，c）中，a和b必然一个是奇数，一个是偶数。

证明　根据基本勾股数组的定义可知（a，b）=1，所以它们不能同时为偶数。若a、b同是奇数，不妨设$a=2m-1$，$b=2n-1$　则

$$a^2+b^2=(2m-1)^2+(2n-1)^2$$
$$=4(m^2+n^2)-4(m+n)+2=c^2,$$

即c^2除以4余数为2　这是不可能的。所以a、b必为一奇一偶。

（2）基本勾股数（a，b，c）中，c必是奇数。

证明　不妨设$a=2m$，$b=2n-1$，则

$$a^2+b^2=(2m)^2+(2n-1)^2$$
$$=4m^2+4n^2-4n+1$$
$$=4(m^2+n^2-n)+1$$
$$=c^2,$$

显然c^2是奇数，所以c也必是奇数。

2．丢番图公式

大约在公元3世纪，大数学家丢番图从不定方程求解的角度出发，系统地研究了勾股数的有关性质。在他的名著《算术》中记载着两个重要公式，现叙述如下：

丢番图公式一　满足下面条件之一的数组a、b和c，必是一组勾股数。

（1）当n是奇数时，

$a=n$，

$b=\frac{1}{2}(n^2-1)$,

$c=\frac{1}{2}(n^2+1)$。

(2) 当n是偶数时,

$a=n$,

$b=\frac{1}{2}n^2+1$,

$c=\frac{1}{2}n^2-1$。

注 可以证明，其中的(1)等价于毕达哥拉斯公式，(2)等价于柏拉图公式。

丢番图公式二 所有的基本勾股数(a, b, c)均可以写为

$$a=2mn,\quad (1)$$
$$b=m^2-n^2,$$
$$c=m^2+n^2。$$

其中$m>n>0$, $(m, n)=1$, 且$2\nmid(m-n)$。同时，符合条件(1)的数组一定是基本勾股数。

证明 首先证明任意勾股数组均可以表示成(1)的形式。由a是偶数可知：存在一个正整数r，使$a=2r$，故$a^2=4r^2$。又由$a^2=c^2-b^2$，得

$$4r^2=(c+b)(c-b)。$$

因为b和c均是奇数 所以$(c+b)$和$(c-b)$均是偶数。

可设 $c+b=2s$, $c-b=2t$。 (2)

于是 $c=s+t$ $b=s-t$。 (3)

将(3)代入(2)得$4r^2=(2s)(2r)$，即

$$r^2=st.$$

又由b、c互素可知s、t也互素．所以根据数论中的一个性质* 可知：s、t均是平方数。即存在两个正整数m、n，使$s=m^2$，$t=n^2$（可设m　n均为正整数）。于是可得

$$a^2=4r^2=4st=4m^2n^2,$$

即$a=2mn$。代入（3）可得$b=m^2-n^2$，$c=m^2+n^2$。根据$b>0$可知$m>n>0$。

现在往证$(m,n)=1$。若存在一个$d\mid m$且$d\mid n$，则$d\mid a$，且$d\mid(m+n)$．又因为$b=m^2-n^2=(m+n)(m-n)$，所以$d\mid b$。根据已知条件$(a,b)=1$，所以$d=1$，即m、n互素。

再证明$2\nmid(m-n)$．根据$(m,n)=1$可知m和n不能都是偶数，现在证它们也不能同是奇数。若不然，则由于$b=m^2-n^2=(m+n)(m-n)$，可知b也是偶数，但是a（偶数）与b互素，矛盾，所以m、n也不能同是奇数．综上m和n只能一个是奇数、一个是偶数。不失一般性，设$m=2k$，$n=2r+1$，则$m-n=2k-(2r+1)=2(k-r)-1$是奇数，所以$2\nmid(m-n)$．

最后证明公式的后半部分，即符合条件（1）的数组一定是基本勾股数组。通过验证很容易证明（1）中的数必是勾股数。现往证$(a,b)=1$。若不然，设p是奇素数，满足$p\mid a$，且$p\mid b$，由$c^2=a^2+b^2$知$p\mid c$。又根据$p\mid b$、$p\mid c$可知$p\mid(b+c)$且$p\mid(b-c)$。但是，$b+c=2m^2$，$b-c=-2n^2$，故$p\mid m^2$且$p\mid 2n^2$。由于p是奇数，故有$p\mid m^2$，$p\mid n^2$，因此$p\mid m$且$p\mid n$。但是$(m,n)=1$，矛盾，

* 即如果$r^2=st$，$(s,t)=1$，则s和t均为平方数。证略。

所以不存在这样的奇素数p。又设$2\mid a$且$2\mid b$，因为$b=m^2-n^2$，且m、n一奇一偶，所以b是奇数，即$2\nmid b$，矛盾。所以a、b也没有偶数公因数，综上得$(a, b)=1$。所以(a, b, c)是一组基本勾股数。

注 如果设

$r=m+n, k=m-n$，则可以得到丢番图公式（二）的等价形式：

$$a=\frac{1}{2}(r^2-k^2),$$

$$b=k,$$

$$c=\frac{1}{2}(r^2+k^2)。$$

其中r、k为互素的奇数，且$r>k$。这一公式是1881年由皮厄莫给出的。

丢番图公式(二)使人们找到了表示勾股数的一般方法，所有特殊的公式都可以通过它的变形求出来。例如，1729年数学家勒格尼根据公式中$m>n>0$的条件，设存在一个正整数d，使$m=d+n$，则

$$a=2n(d+n),$$

$$b=d(d+2n)$$

$$c=a+b^2=b+2n^2。$$

当$d=1$时，就得到了毕达哥拉斯公式；当$n=1$时，就得到了柏拉图公式。

3．其它性质

有了丢番图公式（二），勾股数的许多性质都可以比较容易地证明了。现给出一些例子：

(1) 若 (a, b, c) 是一组基本勾股数，则 $a+c$、$\frac{b+c}{2}$ 和 $\frac{c-b}{2}$ 是完全平方数。

证明　由丢番图公式(二)可得

$$a+c=2mn+(m^2+n^2)=(m+n)^2,$$

$$\frac{b+c}{2}=\frac{(m^2-n^2)+(m^2+n^2)}{2}=m^2,$$

$$\frac{c-b}{2}=\frac{(m^2+n^2)-(m^2-n^2)}{2}=n^2.$$

(2) 若 (a, b, c) 是一组基本勾股数，则 a、b 中必有一个是3的倍数。

证明　若 $a=2mn$ 不是3的倍数，则 m、n 都不是3的倍数。只证当 $m=3u-1$，$n=3v-1$ 时，b 是3的倍数，其余情况可类推。故

$$\begin{aligned}b&=m^2-n^2\\&=(3u-1)^2-(3v-1)^2\\&=9u^2-6u+1-9v^2+6v-1\\&=3(3u^2-2u-3v^2-2v),\end{aligned}$$

所以 b 是3的倍数。

(3) 若 (a, b, c) 是基本勾股数组，则 a，b 中必有一个是4的倍数。

证明　因为 a，b 是一奇一偶，一般设 a 是偶数，则 $a=2mn$。但是 m　n 也是一奇一偶，所以 a 是4的倍数。

(4) 基本勾股数组 $(a$　b，$c)$ 中，必有一个是5的倍数。

证明　可仿 (2) 中的证法，略。

(5) 若 (a, b, c) 是一组基本勾股数，则 abc 是60的倍

数。

证明　根据性质(2)～(4)知a，b和c中有3、4、5的倍数，所以abc是$3\times4\times5=60$的倍数。

(6) 在勾股数中，a、b和c是相继三个自然数的只有3，4和5。

证明　设这类勾股数为$k-1$，k，$k+1$，则

$$(k-1)^2+k^2=(k+1)^2,$$

解之得$k=4$，$k-1=3$，$k+1=5$。

(7) 能构成等差数列的勾股数只有以3、4和5为基本数组的勾股数。

证明　设b为等差中项，则$a+c=2b$，将$c=2b-a$代入$x^2+y^2=z^2$（$x=a$，$y=b$，$z=c$），整理后得

$$3b^2=4ab,$$

即$a:b=3:4$；还可以推出$b:c=4:5$。所以

$$a:b:c=3:4:5.$$

(8) 对于勾股数$a=2mn$，$b=m^2-n^2$，$c=m^2+n^2$，当m、n取相继的正整数时，a，c为相继正整数。例如，

$m=2$，$n=1$时，$(b,a,c)=(3,4,5)$；

$m=3$，$n=2$时，$(b,a,c)=(5,12,13)$；

$m=4$，$n=3$时，$(b,a,c)=(7,24,25)$。

证明　设$m=n+1$，则$a=2mn=2(n+1)n=2n^2+2n$；$c=m^2+n^2=(n+1)^2+n^2=2n^2+2n+1$。所以$c-a=1$。

(9) 适当选取m和n的值，可使a，b和c中一个数并且只能有一个数是平方数。例如，

$m=4$，$n=3$时，$c=25=5^2$；

$m=5$，$n=4$时，$b=9=3^2$；

$m=6$，$n=3$时，$a=36=6^2$

证明略。

(10) 取m、n为相邻的三角形数*时，即

$$m=\frac{(p+1)(p+2)}{2}$$

$$n=\frac{p(p+1)}{2},$$

时，$b=m^2-n^2$是完全立方数。

证明 根据已知得

$$b=m^2-n^2=\frac{(p+1)^2(p+2)^2}{4}-\frac{p^2(p+1)^2}{4}$$

$$=\frac{(p+1)^2(p^2+4p+4-p^2)}{4}$$

$$=(p+1)^3.$$

所以b是完全立方数。

(11) 在勾股数组（a，b，c）中，存在这样的情况：两组或多组不同的勾股数，其中可以有一个数字相同。例如，（3，4，5）与（5，12，13）中有$c_1=a_2=5$；（17，144，145）与（15，8，17）中有$a_3=c_4=17$。图7-1中给出了以一边等于48的全部勾股数作出的直角三角形。实际上，这是一个确定不定方程

$$x^2+y^2=z^2$$

的一类特殊解。即若方程中的x（或y、或z）等于一个常数N时，求出方程的全部解。表7.3给出了当N取最小值时，以N为一边可得勾股数组的情况。其中，T是可得（其中有

---

* 三角形数 定义见本书第八章形数。

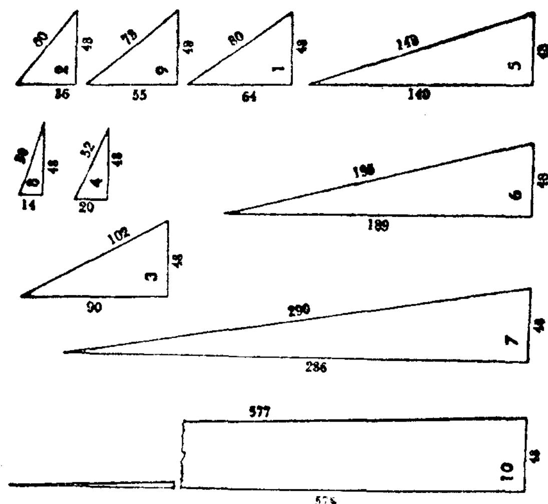


图7-1

一值是N的）勾股数组的个数，N是常值，L是N为直角边长（a或b）时可以得到的三角形个数，H是N为斜边长（c）时可以得到的三角形个数。显然，$T=L+N$。

表7·3　　一边取定值N的勾股数个数表

T	N	L	H	T	N	L	H
1	$3=3$	1	0	51	$2^4\cdot5^6=250000$	45	6
2	$5=5$	1	1	52	$2^4\cdot3^2\cdot7=1008$	52	0
3	$2^4=16$	3	0	53	$2^4\cdot3^2\cdot5=720$	52	1
4	$2^2\cdot3=12$	4	0	54	$2^4\cdot3\cdot5^2=1200$	52	2
5	$3\cdot5=15$	4	1	55	$2^3\cdot3\cdot5^3=3000$	52	3
6	$5^3=125$	3	3	56	$2^{19}\cdot5=$	55	1
7	$2^3\cdot3=24$	7	0	57	$2^{12}\cdot3^2=36864$	57	0
8	$2^3\cdot5=40$	7	1	58	$2^7\cdot3\cdot7=2688$	58	0
9	$3\cdot5^2=75$	7	2	59	$2^7\ 3\cdot5=1920$	58	1
10	$2^4\cdot3=48$	10	0	60	$2^6\cdot3^5=15552$	60	0
11	$2^4\cdot5=80$	10	1	61	$2^{21}\cdot3=$	61	0
12	$2^3\cdot3^2=72$	12	0	62	$2^3\cdot3^2\cdot7^2=3528$	62	0
13	$2^2\cdot3\cdot7=84$	13	0	63	$2^{64}=$	63	0
14	$2^2\cdot3\cdot5=60$	13	1	64	$2^3\cdot3^2\cdot5^2=1800$	62	2
15	$2^{15}=32768$	15	0	65	$3\cdot5^5\cdot13=121875$	49	16
16	$2^6\cdot3=192$	16	0	66	$2^{10}\cdot3^3=27648$	66	0
17	$2^4\cdot3^2=144$	17	0	67	$2^3\cdot3\cdot7\cdot11=1848$	67	0
18	$2^{19}=524288$	18	0	68	$2^3\cdot3\cdot5\cdot7=840$	67	1
19	$2^7\cdot3=384$	19	0	69	$2^2\cdot3\cdot5^2\cdot7=2100$	67	2
20	$2^7\cdot5=640$	19	1	70	$2^{24}\cdot3=$	70	0
21	$3\cdot5^5=9375$	16	5	71	$2^3\cdot3\cdot5\cdot13=1560$	67	4
22	$2^3\cdot3\cdot7=168$	22	0	72	$2^{15}\cdot3^2=294912$	72	0
23	$2^3\cdot3\cdot5=120$	22	1	73	$2^4\cdot3^3\cdot7=3024$	73	0
24	$2^2\cdot3\cdot5^2=300$	22	2	74	$2^4\cdot3^3\cdot5=2160$	73	1
25	$2^9\cdot3=1536$	25	0	75	$2^4\cdot5^9=$	66	9
26	$2^3\cdot5\cdot13=520$	22	4	76	$2^4\cdot3\cdot5^3=6000$	73	3
27	$2^6\cdot3^2=576$	27	0	77	$2^9\cdot3\cdot5=7680$	76	1
28	$2^{10}\cdot3=3072$	28	0	78	$2^{79}=$	78	0
29	$3\cdot5^2\cdot13=975$	22	7	79	$2^{16}\cdot5^2=$	77	2
30	$2^{31}=$	30	0	80	$2^3\cdot5\cdot13\cdot17=8840$	67	13

续

T	N	L	H	T	N	L	H
31	$2^4\cdot3\cdot7=363$	31	0	81	$3\cdot5^{20}=$	61	20
32	$2^4\cdot3\cdot5=240$	31	1	82	$2^6\cdot3^2\cdot7=4032$	82	0
33	$3\cdot5^9=$	25	8	83	$2^6\cdot3^2\cdot5=2880$	82	1
34	$2^2\cdot3\cdot5^3=1500$	31	3	84	$2^6\cdot3\cdot5^2=4800$	82	2
35	$2^3\cdot5\cdot13=1040$	31	4	85	$2^{10}\cdot3\cdot7=21504$	85	0
36	$2^{37}=$	36	0	86	$2^{10}\cdot3\cdot5=15360$	85	1
37	$2^3\cdot3^2\cdot7=504$	37	0	87	$2^4\cdot3^2\cdot7^2=7056$	87	0
38	$2^3\cdot3^2\cdot5=360$	37	1	88	$2^{30}\cdot3=$	88	0
39	$2^3\cdot3\cdot5^2=600$	37	2	89	$2^4\cdot3^2\cdot5^2=3600$	87	2
40	$2^2\cdot3\cdot7\cdot11=924$	40	0	90	$2^3\cdot3^2\cdot5^3=9000$	87	3
41	$2^2\cdot3\cdot5\cdot7=420$	40	1	91	$2^4\cdot5^{11}=$	80	11
42	$2^9\cdot3^2=4608$	42	0	92	$2^{19}\cdot3^2=$	92	0
43	$2^4\cdot5^5=50000$	38	5	93	$2^9\ 3^5=124416$	93	0
44	$2^2\ 3\cdot5\cdot13=780$	40	4	94	$2^4\cdot3\cdot7\cdot11=3696$	94	0
45	$2^7\cdot3^3=3456$	45	0	95	$2^4\cdot3\cdot5\cdot7=1680$	94	1
46	$2^{16}\cdot3=196608$	46	0	96	$2^{97}=$	96	0
47	$2^{10}\cdot3^2=9216$	47	0	97	$2^7\cdot3^2\cdot7=8064$	97	0
48	$2^7\cdot5^3=16000$	45	3	98	$2^4\cdot3\cdot5\cdot13=3120$	94	4
49	$2^6\cdot3\cdot7=1344$	49	0	99	$2^7\cdot3\cdot5^2=9600$	97	2
50	$2^6\cdot3\cdot5=960$	49	1	100	$2^{34}\cdot3=$	100	0

表7.4中给出了一些大得惊人的结果，例如，当（a，b，c）中的某一个值等于$2^{330}\cdot3^{44}\cdot5^5\cdot7^{15}$时，可以得到$10^7$个勾股数组。其中，有一条直角边长相同的有9999995个，一条斜边相同的有5个。

表7·4　　$T \geq 100$时的某些勾股数个数表

T	N	L	H
100	$2^{34}\cdot 3=$	100	0
200	$2^{10}\cdot 3^3\ 5=138240$	199	1
300	$2^{9}\cdot 3^2\cdot 5^3=576000$	297	3
400	$2^{45}\cdot 3\cdot 7=$	400	0
500	$2^{19}\cdot 3\cdot 5\cdot 7=$	499	1
600	$2^{601}=$	600	0
700	$2^{234}\cdot 3=$	700	0
800	$2^{21}\cdot 3^6\cdot 5=$	799	1
900	$2^4\cdot 3^2\cdot 5^8\cdot 7=$	892	8
1000	$2^{10}\cdot 3^2\cdot 5^3\cdot 7=$	997	3
500000	$2^{19}\cdot 3^6\cdot 5\cdot 7^5\cdot 11^3\cdot 19\cdot 23$	499999	1
1000000	$2^{9991}\cdot 5^{50}$	999950	50
1500000	$2^{180}\cdot 3^2\cdot 5^{278}\cdot 7$	1499722	78
2000000	$2^{1000}\cdot 3^{14}\cdot 5\cdot 7^{11}$	1999999	1
2500000	$2^{19}\cdot 3^6\cdot 5^3\cdot 7^5\cdot 11^2\cdot 19\cdot 23\cdot 31$	2499997	3
3000000	$2^{271}\cdot 3^6\ 5^{426}$	2999574	26
3500000	$2^{19}\cdot 3^6\cdot 5\cdot 7^5\cdot 11^3\cdot 13\cdot 19^3\cdot 23$	3499996	4
4000000	$2^{6634}\cdot 3^{33}\cdot 7\cdot 11$	4000000	
4500000	$2^{19}\cdot 3^6\cdot 5^5\cdot 7_3\cdot 11\cdot 19\cdot 23\cdot 31\cdot 43$	4499995	5
5000000	$2^{2325}\cdot 3^{119}\cdot\cdot 5\cdot 7$	4999999	1
5500000	$2^{19}\cdot 3^5\cdot 5^6\cdot 7^3\cdot 19\cdot 19\cdot 23$	5499994	6
6000000	$2^{1279}\cdot 3^9\cdot 7^9\cdot 11^6$	6000000	0
6500000	$2^{97}\cdot 3^8\cdot 5^{116}\cdot 13^6$	6498020	1980
7000000	$2^{117}\cdot 3^{30}\cdot 5^{98}\cdot 7^2$	6999902	98
7500000	$2^{1230}\cdot 3^{74}\cdot 5^{11}\cdot 7$	7499989	11
8000000	$2^{79}\cdot 3^6\cdot 5^{33}7^6\cdot 13\cdot 17$	7999699	01
8500000	$2^{7210}\cdot 3^{65}\cdot 7\cdot 11$	8500000	0
9000000	$2^{2722}\cdot 3^{1653}$	9000000	0
9500000	$2^{19}\cdot 3^9\cdot 5^3\cdot 7^6\cdot 11^5\cdot 13\cdot 19\cdot 23$	9499990	10
10000000	$2^{330}\cdot 3^{44}\ 5^5\ 7^{15}$	9999995	5

对于(a, b, c)中某一值固定后可得到的勾股数组的情况，可由下面的公式给出：

设勾股数中的某一值确定为N，它的因数分解式为

$$N=2^{a_0}\cdot p_1^{a_1}\cdot p_2^{a_2}\cdots p_n^{a_n},$$

则以N为一直角边长的勾股数组的个数为

$$L=\frac{(2a_0-1)(2a_1+1)\cdots(2a_n+1)-1}{2};$$

如果设N的因数分解式为

$$N=2^{a_0}\cdot p_1^{a_1}\cdots p_n^{a_n}q_1^{b_1}\cdots q_r^{b_r},$$

其中p_i是$4x-1$形式的奇素数，q_i是$4x+1$形式的奇素数，则以N为斜边长的勾股数组的个数为

$$H=\frac{(2b_1+1)(2b_2+1)\cdots(2b_r+1)-1}{2}.$$

(12) 还有一些可以给出部分勾股数组的公式，例如：

$a=3m^2-2m$,

$b=4m^2-6m+2$, ($m>1$，且是奇数)

$c=5m^2-6m+2$;

以及

$a=6m^2-2m$,

$b=8m^2-6m+1$, (m$\geqslant$2，且是偶数)

$c=10m^2-6m+1$.

§7.3 推广——费尔马大定理

关于勾股数的推广，可以产生出许多重要的结果。限于

篇幅，这里就不逐一介绍了。仅给出一个最著名的推广：费尔马大定理的产生和发展。

1621年，费尔马在阅读丢番图的《算术》一书时，由方程

$$x^2+y^2=z^2$$

想到了更一般的不定方程

$$x^n+y^n=z^n \qquad (n\text{为大于2的正整数})$$

的整数解问题。他在《算术》第二册的1页空白处写下这样一段话："要把一个立方数分为两个数的立方和，一个四次方数分为两个数的四次方和；或者一般地，把一个大于2的乘方数分为两个同指数幂的乘方数的和，都是不可能的。对于这个问题，我发现了一种很巧妙的证法，可惜这里的地方太小，写不下。"费尔马去世后，人们在他的图书室找到了这本书，并把费尔马的这段话公诸于世。但是，没有人见过他的"巧妙证法"，从此数学家们就把它作为"猜想"展开了证明，一般称之为费尔马大定理，或费尔马最后定理。

费尔马猜想可以变换成另一个等价的问题，即如果$n=4$时，以及n等于任一个奇素数p时，

$$x^n+y^n=z^n$$

没有正整数解，那么它对任何正整数n均无正整数解。

早在公元972年，阿拉伯人阿尔柯旦弟就认为$n=3$时，$x^3+y^3=z^3$没有正整数解。但是，他的证明有误。1770年，欧拉也证明了这一特例，但是仍不完美。$n=4$的情况是莱布尼兹和欧拉各自独立解决的。1823年，勒让德证明了$n=5$的情况，两年后狄里克雷再次独立地证明了这一结果。1840年，拉美证明了$n=7$的情况。

19世纪，德国数学家库默深入研究了费尔马猜想，他通过建立崭新的数学理论——理想数论，使猜想的证明得到重大突破。1844年库默证明：当奇素数$p<100$时，除了$p=37$、59和67以外，费尔马猜想成立。$p=37$时的情况是1892年由米里曼诺夫解决的。1941年D.H.莱赫默与E.莱赫默共同证明：如果x、y、z都与p互素，则当$p<253747889$时，$x^p+y^p=z^p$无正整数解。1944年，谢尔弗力基等人证明：当$p<4002$时，一般情况均无正整数解。1977年，瓦格斯塔夫等人借助大型计算机证明：当$2<p<125000$时，无正整数解。

在漫长的岁月中，历代数学家的辛勤劳动使人们感到：要想解决这个猜想绝不象费尔马说的那样轻易，大概当时费尔马得到了错误的结果或根本没有证明。事实上，费尔马大定理的难度不下于任何数学难题，甚至使许多数学大师们怀疑现有的知识是否能够胜任这项证明。但是，1983年问题出现了极大的转机。一位年仅29岁的西德人法尔廷斯天才地证明了1922年英国数学家莫德尔提出的一个关于“二元有理系数多项式解的个数”的猜想，通过这一证明可以得到结论：当$n\geqslant4$时，

$$x^n+y^n=z^n$$

至多只有有限组正整数解。这一结果引起了数学界的震惊，有人认为这可能是“近百年来解决的最重要的数学问题，至少对数论来讲，已达到了本世纪的顶峰。

第八章　形　　数

自然依据精巧的蓝图所安排的万物，不论是单独的还是整体的，都象是被按照数来创造一切的先知和理性所挑选出来并排列成序的，…它们是真实的；的确，是真正真实的，永恒的。

——尼可马修斯

§8.1　“圣数”之谜

“形数”是一个笼统的概念，它很难用严格的数学语言定义出来。这类问题产生于数的几何表示法，是古希腊数学思想的一个重要组成部分。根据博学者亚历山大记载，古希腊的毕达哥拉斯学派认为：一切几何图形都是由数产生的。即“从数产生出点，从点产生出线，从线产生出平面图形，从平面图形产生出立体图形，……。”

例如，若以数字对应空间的点，则“1”是点，“2”是线（两点可以连成一条线），“3”是平面（三点可以确定一个平面），“4”是立体（不在同一平面上的四个点可以作成一个四面体），见图8-1。这个例子也说明，在古希腊时期，人们是用“圆点”来记录数的。

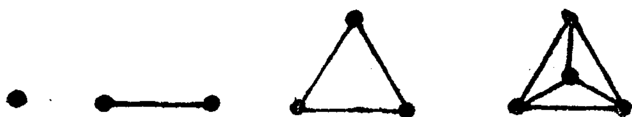


图8-1

注 事实上，最早用"圆点"表示数的还有许多古人。例如，远古时代我国学者惊人地给出了世界上第一个纵横图(西方称为幻方)，其中用实心点表示偶数，称为阴性数；空心点表示奇数，称为阳性数。见图8-2。

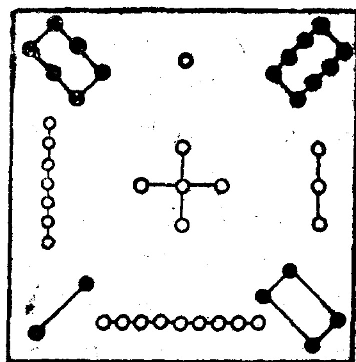


图8-2

以这个观点为基础，毕达哥拉斯研究了数与形的奇妙联系，最早提出了著名的"k角形数"问题。据记载，有一次一个商人问毕达哥拉斯能教他什么知识，毕达哥拉斯说："我来教你怎样计数吧？"商人说："我早就会计数了"。毕达哥拉斯问："你是怎样计数的？"于是商人开始数道："1，2，3，4，…"，毕达哥拉斯说："不要数了，你所说

的4其实是10，它是一个完全三角形数，是我们的标志和指令。”这句话说得令人迷惘，它的内涵是什么呢？

原来毕达哥拉斯学派十分崇拜数字“4”，它被认为代表四种元素：水，火，气，土。而10＝1＋2＋3＋4，所以他止住了商人的读数，自认为这已足够“包罗万象”了。再请看毕达哥拉斯学派的一段祷文：

“创造诸神和人类的神圣的数啊，愿您赐福我们！啊！圣洁的‘4’啊，您孕育着永流不息的创造源泉！因为您起源于纯洁而深奥的‘1’，渐次达到圣洁的4，然后生出圣洁的‘10’，它为天下之母，无所不包，无所不属，首出命世，永不偏倚，永不倦怠，成为万物之钥”。

其实，毕达哥拉斯喜爱10的主要根源是他们发现了“形数”的奥秘。因为用10个圆点按照递增的规律，恰好可以堆垒成一个三角形（见图8-3中的T_4），所以把它称为完全三角形数。图8-3给出了前几个三角形数，它们是T_i：

1，3，6，10，15，…

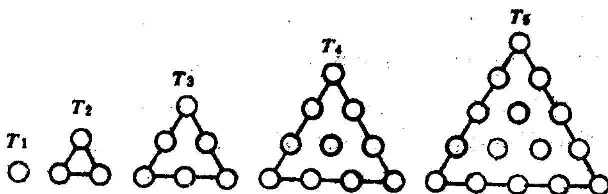


图8-3

那么，数字“4”的数学本源是什么呢？这是因为除了所谓“万物的本源”1之外，4是第一个完全平方数，即$4=2^2$。请看图8-4，这里给出了一系列完全平方数（或称四角形数）的对应图形。这些数字是s_i：

1，4，9，16，25，…

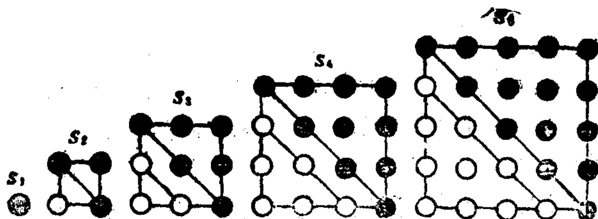


图8-4

它们组成了一个个规整的正方形，因此最受毕达哥拉斯学派推崇。

另外，毕达哥拉斯学派还发现了平方数与三角形数之间的关系，即每一个平方数都等于与它同阶的三角形数与前一阶的三角形数之和.从图8-4中，通过实心点和空心点的组合，我们可以清楚地看到这个关系.

注 所调"阶数"是指k角形数在数列中的序数（或位置）。例如，任一三角形数T_i的阶数就是i.

应当指出，"形数"是毕达哥拉斯学派关于"数是万物的本源"这一学说的一个重要组成部分，毕达哥拉斯是用它去说明"一切形体都是由数派生出来的"这一哲理。虽然他们的观点存在着许多不当之处，但是，从数学角度而言，毕达哥拉斯却奉献出一颗璀璨的数字明珠——形数。

§8.2 形数合一

形数可以按照平面图形、立体图形以及高维空间•图形

• 在数学中，一般地说直线可构成一维空间，平面可构成二维空间，立体可构成三维空间。高于三维的空间无法作出图形，但是可以求出它的数学性质。

表8-1 k角形数表

K角形数	阶数				
三角形数					
四角形数					
五角形数					
六角形数					
七角形数					
八角形数					

分类。上节给出的三角形数和四角形数都是平面中的形数，它们一般称为k角形数。表8.1中给出了前几项k角形数，它们排列整齐、规律，十分有趣。下面我们就从k角数开始，介绍一下形数的数学性质和它们之间的关系。

1．k角形数

从表8·1中，我们可以发现k角形数的排列规律。例如，我们把三角形数在同一排上的“点”累加起来，得到结果：

第一个数：1，

第二个数：1+2，

第三个数：1+2+3，

……

第n个数：$1+2+\cdots+n$。

它们恰是递增的自然数之和。根据自然数求和公式，可以得到任意一项的三角形数的通项公式为

$$T_r=\frac{r(r+1)}{2}.$$

例如，$r=5$时，$T_4=4(4+1)/2=15$，恰好是第5个三角形数。

从上一节中可知，毕达哥拉斯给出了四角形数与三角形数之间的关系（见图8-4）。由此可以推出四角形数的通项公式：

$$S_r=T_r+T_{r-1}=\frac{r(r+1)}{2}+\frac{r(r-1)}{2}$$

$$=\frac{r(r+1+r-1)}{2}=r^2.$$

五角形数的通项公式也可以由此三角形数和四角形数之

间的关系导出。从图8-5中可以推测：任一个五角形数等于与它同阶的四角形数与前一阶的三角形数之和，即

$$P_r=S_r+T_{r-1}=r^2+\frac{r(r-1)}{2}$$

$$=\frac{r(3r-1)}{2}.$$

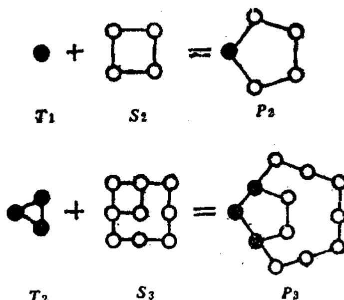


图8-5

一般地可以证明：任一个k角形数（记为p_k^r）等于它同阶的$(k-1)$角形数（p_{k-1}^r）与前一阶的三角形数（p_3^{r-1}）之和，即

$$p_k^r=p_{k-1}^r+p_3^{r-1}=\frac{r\,[(r-1)k-2(r-2)]}{2}.$$

其中的k表示角数，r表示阶数（即p_k^r表示第r个k角形数）。表8·2中给出了它们的部分结果和通项公式。

根据k角形数的通项公式可以得到下面一些有趣的性质：

（1）如果正整数n满足关系：

$$n\times 8(k-2)+(k-4)^2=\text{一个平方数},$$

则n是一个k角形数。否则n不是一个k角形数。

表8·2　　k角形数的通项公式表

名　称	阶数r									
	1	2	3	4	5	6	7	8	…	r
三角形数	1	3	6	10	15	21	28	36	…	$r(r+1)/2$
四角形数	1	4	9	16	25	36	49	64	…	r^2
五角形数	1	5	12	22	35	51	70	92	…	$r(3r-2)/2$
六角形数	1	5	15	28	45	66	91	120	…	$r(2r-1)$
七角形数	1	7	18	34	55	81	112	148	…	$r(5r-3)/2$
八角形数	1	8	12	40	65	96	113	176	…	$r(3r-2)$
…	……								…	…
k角形数	1	k	$3(k-1)$	$2(3k-4)$	$5(2k-3)$	$3(5k-8)$	$7(3k-5)$	$4(7k-12)$		$(r/2)[(r-1)k-2(k-2)]$

这一性质可以根据k角形数的通项公式直接导出。例如，我们要验证数字45是否为六角形数。因为

$$45\times 8(6-2)+(6-4)^2=1440+4=38^2,$$

所以45是一个六角形数。

(2) 一个k角形数n的阶数

$$r=\frac{R+(k-4)}{2(k-2)},$$

其中$R=\sqrt{8n(k-2)+(k-4)^2}$。

证明　根据性质（1）及k角形数的通项公式可得

$$n\times 8(k-2)+(k-4)^2$$

$$=\frac{r\left[(r-1)k-2(r-2)\right]}{2}8\times(k-2)+(k-4)^2$$

$$=(2rk-4r-k+4)^2.$$

设$R=2rk-4r-k+4$，解出r得

$$r=\frac{R+(k-4)}{2(k-2)},$$

又由上述推导过程可得

$$R=\sqrt{8n(k-2)+(k-4)^2}.$$

例如，对于六角形数45，$R=38$，所以

$$r=\frac{38+(6-4)}{2(6-2)}=\frac{40}{8}=5.$$

即45处于六角形数数列中的第5位（见表8·2所示）。

（3）如果一个正整数的数字根是

2，4，5，7，8，

则它一定不是一个三角形数；如果它的数字根是

1，3，6，9，

则它可能是三角形数，也可能不是三角形数。

例如，数字79的数字根为7（即$7+9=16$，$1+6=7$，所以数字根为7），所以它不是一个三角形数。而54的数字根为$5+4=9$，因此用这种方法不能判定它是否为三角形数。但是根据性质（1）：

$$54\times 8(3-2)+(3-4)^2=433,$$

不是一个完全平方数，所以54也不是一个三角形数。

（4）设$S=x^2$是一个四角形数（即完全平方数），如果

x^2+1也是一个四角形数，即

$$8x^2+1=y^2,^{•}$$

则$S=x^2$也是一个三角形数。

证明　根据性质(1)可知，任一个k角形数乘以$8(k-2)$，再加上$(k-4)^2$都等于一个平方数。对于三角形数，即$k=3$时，有结论：一个三角形数乘以$8(3-2)=8$，再加上$(3-4)^2=1$，必等于一个平方数。所以，如果能找到一个平方数，它乘以8，再加上1之后仍然是一个平方数，则根据性质(1)，它也必然是一个三角形数。这实际上是一类不定方程（即佩尔方程）$8x^2+1=y^2$的求解问题，表8·3中给出了几组解。

表8·3　　既是平方数又是三角形数的数表

佩尔方程$8x^2+1=y^2$的解	三角形数	三角形数的阶数	平方数的阶数
$8\cdot1^2+1=3^2$	1	1	1
$8\cdot6^2+1=17^2$	36	8	6
$8\cdot35^2+1=99^2$	1225	49	35
$8\cdot204^2+1=577^2$	41616	288	204
$8\cdot1189^2+1=3363^2$	1413721	1681	1189
$8\cdot6930^2+1=19601^2$	48024900	9800	6930
$8\cdot40391^2+1=114243^2$	1631432881	57121	40391

(5) 数列

0，1，6，35，204，…，u_n，…中的数的平方既是三角形数，又是平方数。它的递推关系是$u_{n+1}=6u_n-u_{n-1}$。

• 这是一个不定方程，在数论中习惯把这类方程（即$x^2-Dy^2=1$）称为佩尔方程。实际上佩尔并没有研究过这类方程，它是费尔马最早提出的一个求解问题。但是18世纪欧拉在著作中误把它称为佩尔方程，而且欧拉的名气又太大了，因此得以误称至今。

这一结果已在表8·3中见到。

注 这一数列也是斐波那契数列的一个推广形式，它的通项公式为：

$$u_n=\left[\frac{(1+\sqrt{2})^{2x}-(1-\sqrt{2})^{2x}}{2\sqrt{2}}\right]^2.$$

(6) 6是在小于10^{660}的正整数中唯一的一个平方之后仍然是三角形数的三角形数。

这一问题的证明需要用到佩尔方程解的有关知识，在这里就不介绍了。

(7) 55，66和666是小于10^{30}的正整数中仅有的三个数字完全重复的三角形数。

(8) 存在着这样一些三角形数对，它们的和与差仍然是三角形数。表8·4给出了几组有趣的结果。

表8·4　　和与差均是三角形数的三角形数表

第一个三角形数 $F=x(x+1)/2$	第二个三角形数 $S=y(y+1)/2$	阶数 x	阶数 y	$F+S=z(z+1)/2$	$F-S=v(v+1)/2$	阶数 z	阶数 v
21	15	6	5	36	6	8	3
171	105	18	14	276	66	23	11
990	780	44	39	1770	210	59	20
3741	2145	86	65	5886	1596	108	56
2185095	1747515	2090	1869	3932610	437580	2804	935

(9) 除了数字1之外，数字210和40755既是三角形数，又是五角形数。一般地，除了数字1之外，是否存在一个数字，它既是n角形数，又是m角形数（$m\neq n$）？这是一个十分有趣的问题，读者可自行思考。

(10) 仅当$2r+1=3u$时，三个连续的三角形数之积

$$p_3^{r-1}\cdot p_3^r\cdot p_3^{r+1}$$

是一个平方数。这里u是数列

$$1,\ 3,\ 17,\ \cdots,\ u_n=6u_{n-1}-u_{n-2},\ \cdots$$ 中的任一项。

例如，当$u=3$时，可得三个三角形数6、10和15，它们的乘积$6\times10\times15=900=30^2$，恰好是一个平方数。当$u=17$时，$r=25$，则

$$p_3{}^{24}\cdot p_3{}^{25}\cdot p_3{}^{26}=300\cdot325\cdot351=5850^2。$$

(11) 自然数的立方和等于三角形数的平方，即

$$1^3+2^3+\cdots+n^3=(1+2+\cdots+n)^2=\left[\frac{r(r+1)}{2}\right]^2.$$

(12) 任何自然数均可以用不超过k个k角形数之和来表示。

(13) 图8-6中给出了k角形数之间的一些有趣的结果。我们将图形与公式对应起来，充分体现了数与形之间的微妙关系。公式中的p_k^r表示第r个k角形数；f_1^r表示数字r，反映在图形上就是r个点。从图8～6中，还可以找出许多k角形数之间的联系，在此就不一一说明了。请读者细细品味。

还有一些有趣的结果，如三角形数与完全数、勾股数的关系，等等，我们已在前几章有所介绍，在此就不赘述了。

2．立体数与四维形数

立体数（也称k面体数）与四维形数，乃至更高维形数都可以通过k角形数的推广得到。请看图8-7，这里给出了四面体数，它们显然可以通过累加三角形数得到。我们将第四个四面体数分解开来，可以清楚地看到，它就象将一系列三角

图形	关系式	图形	关系式
	$\frac{r(r+1)}{2}+(r+1)=\frac{(r+1)(r+2)}{2}$ $p_3^r+f_1^{r+1}=p_3^{r+1}$		$4\frac{r(r+1)}{2}+(r+1)=(r+1)(2r+1)$ $4p_3^r+f_1^{r+1}=p_6^{r+1}$
	$2\frac{r(r+1)}{2}=r(r+1)$ $2p_3^r=r(r+1)$		$6\frac{r(+1)}{2}+(r+1)=(r+1)(3r+1)$ $6p_3^r+f_1^{r+1}=p_8^{r+1}$
	$r^2+(2r+1)=(r+1)^2$ $p_4^r+f_1^{2r+1}=p_4^{r+1}$		$3\frac{r(r+1)}{2}+\frac{(r+1)(r+2)}{2}=\frac{(2r+1)(2r+2)}{2}$ $3p_3^r+p_3^{r+1}=p_3^{2r+1}$
	$8\frac{r(r+1)}{2}+1=(2r+1)^2$ $8p_3^r+1=p_4^{2r+1}$		$14\frac{2\times3}{2}+2\frac{3\times4}{2}+1=\frac{10\times11}{2}$ $14p_3^2+2p_3^3+1=p_3^{10}$

图形	关系式	图形	关系式
	$3\frac{r(r+1)}{2}+(r+1)=\frac{(r+1)(3r+2)}{2}$ $3p_3^r+f_1^{r+1}=p_5^{r+1}$		$2\frac{r(r+1)}{2}+(r+1)^2=(r+1)^2$ $2p_3^r+f_1^{r+1}=p_4^{r+1}$

图8-6

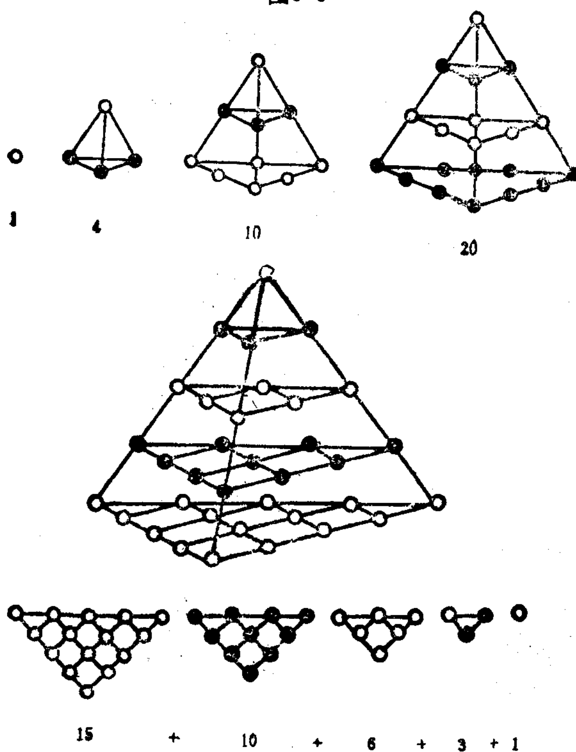


图8-7

形（数）由小到大一层层摞起来一样。若用P_3^r表示四面体数，则有

$$P_3^r=p_3^1+p_3^2+\cdots+p_3^r=\frac{r(r+1)(r+2)}{6}。$$

图8-8给出了五面体系（或称四棱锥数）。同四面体数与三角形数的关系类似，它也与四角形数存在着明显的关系：

$$P_4^r=p_4^1+p_4^2+\cdots+p_4^r=\frac{r(r+1)(2r+1)}{6}。$$

这实际上是自然数的平方和，因为任一个$p_4^r=r^2$。

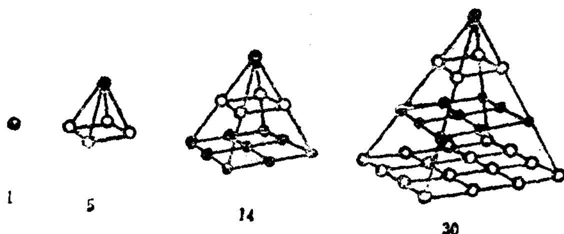


图8-8

根据三角形数与四角形数的关系，不难得到结论：任一个五面体数都等于与它同阶的四面体数与前一阶的四面体数之和。即

$$p_4^r=p_3^r+p_3^{r-1}.$$

一般地，可以证明：任一个k面体数（p_k^r）都等于与它同阶的（$k-1$）面体数（p_{k-1}^r）与前一阶的四面体数（P_3^{r-1}）之和。即

$$P_k^r=P_{k-1}^r+P_3^{r-1}$$
$$=\frac{(r+1)(2p_k^r+r)}{6}$$

$$=\frac{r(r+1)\ [(r-1)k-(2r-5)]}{6}.$$

表8·5给出了k面体数的一些结果和通项公式。

表8·5　　　　k面体数的通项公式表

名称	阶数									
	1	2	3	4	5	6	7	8	…	r
四面体数	1	4	10	20	35	56	84	120	…	$r(r+1)(r+2)/6$
五面体数	1	5	14	30	55	91	140	204	…	$r(r+1)(2r+1)/6$
六面体数	1	6	18	40	75	126	196	288	…	$r^2(r+1)/2$
七面体数	1	7	22	50	95	161	252	372	…	$r(r+1)(4r-1)/6$
八面体数	1	8	26	60	115	196	308	456	…	$r(r+1)(5r-2)/6$
九面体数	1	9	30	70	135	231	364	540	…	$r(r+1)(2r-1)/2$
k面体数	1	$k+1$	$2(2k-1)$	$10(k-1)$	$5(4k-5)$	$7(5k-7)$	$28(2k-3)$	$12(7k-11)$	…	$[r(r+1)/6]\ [(r-1)k-(2r-5)]$

k面体数还有一些有趣的性质。例如，在五面体数中只有唯一的一个平方数：

$$P_4^{24}=\frac{24(24+1)(48+1)}{6}=4900=70^2;$$

四面体数中仅有两个平方数：

$$P_3^2=\frac{2(2+1)(2+2)}{6}=4=2^2$$

和140^2，等等。

类似地，我们还可以给出四维形数乃至更高维形数的数

学公式，但是却无法给出它们的图形了。数学毕竟不能完全依赖于直观表述，抽象思维是它最重要的特征之一。这时我们要想很好地理解数学原理，就需要运用“空间想象能力”了。表8.6是四维形数的部分结果和通项公式。

表8·6　　四维形数的通项公式表

名　称	阶数 1	2	3	4	5	6	7	8	…	r
第一四维形数	1	5	15	35	70	126	210	330	…	$r(r+1)(r+2)(r+3)/4!$
第二四维形数	1	6	20	50	105	196	336	540	…	$r(r+1)^2(r+1)/12$
第三四维形数	1	7	25	65	140	266	462	750	…	$r(r+1)(r+2)(3r+1)/4!$
第四四维形数	1	8	30	80	175	336	588	960	…	$r^2(r+1)(r+2)/6$
第五四维形数	1	9	35	95	210	406	714	1170	…	$r(r+1)(r+2)(5r-1)/4!$
第六四维形数	1	10	40	110	245	476	840	1380	…	$r(r+1)(r+2)(6r-2)/4!$
第K四维形数	1	$(K+2)$	$5K$	$5(3K-2)$	$35(K-1)$	$14(5K-6)$	$42(3K-4)$	$30(7K-10)$		$r(r+1)(r+2)[(r-1)(K-2)+4]/4!$

n维形数的通项公式如下：

$$f^r_{n,s}=\frac{(rs+n-s)(r+n-2)!}{n!\,(r-1)!}.$$

其中，n是维数，s是类数（即第n维形数从小到大的分类数。例如，k角形数中$s=1$类的是三角形数，$s=2$类的是四角形数，等等），r是阶数。例如，当$s=1$时，

$$f_{n,1}^{r}=\frac{(n+1)(n+2)\cdots(n+r-1)}{(r-1)!}.$$

它可以给出三角形数、四面体数、第一四维形数，…，等等。比如，$n=2$时，

$$\begin{aligned}f_{2,1}^{r}&=\frac{(2+1)(2+2)\cdots(2+r-1)}{(r-1)!}\\&=\frac{3\cdot4\cdot\cdots\cdot(r-1)r(2+r-1)}{1\cdot2\cdot3\cdot\cdots\cdot(r-1)}\\&=\frac{r(r+1)}{2}.\end{aligned}$$

恰好是三角形数。

读者一定会觉得：形数是数论中最独特的一类数字！它一反数论中严格的抽象性，在几何学中辟出一个“形数合一”的新领域，使人耳目一新，形成了一个丰富严整的数学体系。

封面设计：冯贵才

科技新书目：205-365

ISBN 7-5308-0453-7/O·26

定　价：　2.10元